FSB
FINANCIAL
STABILITY
BOARD

# Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector

10 October 2025

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

# Table of Contents

# Executive Summary

Artificial intelligence (AI) is reshaping the financial sector, driving efficiency and innovation. AI has the potential to improve efficiency, help with regulatory compliance, enable advanced data analytics and produce more personalised financial products. However, the FSB's 2024 AI report identified several vulnerabilities, including third-party dependencies, market correlations, cyber risks, and challenges in model risk and governance, which may have implications for financial stability. At the request of the South African G20 Presidency, this report examines how financial authorities can monitor AI adoption and assess related vulnerabilities. It builds on the FSB's 2024 report and incorporates findings from a member survey on AI monitoring approaches, interviews with member authorities, publicly available information and stakeholder outreach.

This report identifies a range of indicators to support monitoring of AI adoption and related vulnerabilities in the financial system, including direct indicators and proxy indicators. These can be collected through surveys, outreach, supervisory engagement with regulated entities, leveraging publicly available and vendor data, and existing supervisory frameworks.

While financial authorities have made progress in understanding AI use cases and their benefits and vulnerabilities, their monitoring efforts are still at an early stage. Respondents to the member survey highlighted challenges such as a lack of agreed definitions for AI, difficulties in ensuring comparability across jurisdictions, challenges in assessing the criticality of AI services, as well as the cost and scope of monitoring.

Many authorities have plans to enhance their AI-related data collection initiatives. This report highlights approaches to support these efforts, such as simplifying surveys, fostering data sharing across domestic authorities, and using indicators identified in this report to improve monitoring efforts. Additionally, AI tools can support monitoring and risk management by enhancing fraud detection, improving cyber defences, and enabling more effective supervisory frameworks. The mapping of indicators to specific vulnerabilities, however, remains challenging. Certain vulnerabilities, such as third-party dependencies, market correlations, cyber risks, and model governance challenges, are particularly difficult to monitor due to limited data availability, lack of transparency, and the evolving nature of AI systems. Monitoring efforts could benefit from exploring cost-effective approaches that are representative, mapped to identified vulnerabilities, timely, and aligned, where possible, with relevant standards.

Building on the FSB's 2024 report, which identifies third-party dependencies and service provider concentration as key vulnerabilities, this report examines recent developments that could have implications for financial institutions' (FIs) reliance on a small number of third-party service providers. These developments highlight the importance of monitoring the role of service providers in supporting FIs' operations and addressing potential vulnerabilities in the AI supply chain. The report includes a case study on this issue, relating to generative AI (GenAI), noting that while FIs appear to be cautiously adopting GenAI with apparently limited use for critical functions and critical operations so far, FIs are also exploring new use cases. Third-party service providers play a critical role in FIs' development and deployment of effective GenAI applications. However, such relationships may also expose FIs to operational vulnerabilities and the growing use of GenAI could lead to critical third-party dependencies. The case study highlights the layered nature of the GenAI supply chain and the vulnerabilities that can arise from adoption

trends, concentration, and vertical integration. Drawing on the FSB's third-party risk management toolkit, the case study highlights considerations for authorities monitoring GenAI and suggests potential indicators for assessing criticality, concentration, substitutability and the systemic relevance of third-party AI service providers.

The report concludes with the following considerations for the FSB, standard setting bodies (SSBs) and national financial authorities:

- National authorities are encouraged to enhance their monitoring approaches by leveraging the potential indicators presented in this report, collaborating with domestic stakeholders to formalise metrics, enhancing engagement with regulated FIs, exploring AI tools to both monitor and mitigate vulnerabilities, and promoting greater data sharing across domestic authorities.

- The FSB and relevant SSBs should continue to support these efforts by facilitating cross-border cooperation, including through sharing information, experiences, and good practices, and by working towards greater alignment in taxonomies and indicators where feasible.

- The FSB and relevant SSBs are encouraged to continue monitoring AI developments and addressing data gaps as appropriate, working towards a comprehensive approach to understanding AI adoption in the financial sector and related vulnerabilities.

The findings of this report highlight the importance of monitoring vulnerabilities associated with AI adoption. These findings will help inform future FSB work on AI.

# 1. Introduction

The Financial Stability Board's (FSB) 2024 report on the financial stability implications of AI reviewed recent advancements in the technology and its increasing adoption in the financial system.[1]

Though the financial sector has long used AI tools, recent changes in the availability and capability of AI models have the potential to transform the financial system by driving innovation, improving efficiency, and enhancing resilience. It can streamline operations, support regulatory compliance, enable advanced data analytics, and facilitate the development of more personalised financial products and services. Its adoption within the financial system could be both extensive and rapid, driven by the significant opportunities it offers to FIs and their customers. However, as highlighted in the FSB 2024 report, such rapid adoption may introduce financial stability vulnerabilities. This report, therefore, focusses on the importance of monitoring these vulnerabilities that could emerge in the financial system, with the aim of safeguarding financial stability while creating an environment that supports safe and sound innovation.

The report focused on the key drivers of AI uptake and identified prevalent use cases. It also highlighted potential vulnerabilities in the financial sector that could be amplified by AI, including: (i) third-party dependencies and service provider concentration; (ii) market correlations; (iii) cyber risks; and (iv) model risk, data quality, and governance. The report noted that GenAI could increase financial fraud and the ability of malicious actors to generate and spread disinformation in financial markets.[2] In addition, the report noted that misaligned AI systems – those that are not calibrated to operate within legal, regulatory, and ethical boundaries – could also engage in behaviour that harms financial stability.[3] The report called for national financial authorities and international bodies to enhance their monitoring of AI developments, assess whether financial policy frameworks are adequate, and enhance their regulatory and supervisory capabilities, including by using AI-powered tools.

Since the publication of the 2024 FSB report, several notable developments have emerged in the AI ecosystem. These include: (i) advancements in AI models, such as the introduction of high-performance, lower-cost, open-weight models,[4] and the development of multi-step "reasoning" models;[5] (ii) the entry of new providers specialising in open-weight models; (iii) developments in the hardware market, such as increased competition; and (iv) vertical

[1] FSB (2024), *The financial stability implications of artificial intelligence*, November.

[2] Generative AI refers to systems that create new content, such as text, images, or code, based on patterns in the data they were trained on.

[3] The 2024 FSB report also noted that 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. However, this report does not cover these issues as their financial stability implications remain unclear.

[4] Open weight models disclose the learned parameters of an AI model, such as weights and biases, enabling developers to fine-tune the model for specific applications. Open source models may go further by providing the full training code and in some cases documentation or access to training data or its composition. This distinction matters because open weight models typically offer faster deployment and cost savings through existing infrastructure, while fully open source models provide greater customisation potential but require more significant technical investment. Models often exist on a spectrum. Some might share their weights but restrict usage, while others may be open source but keep training data proprietary. See Open Source Initiative's definition.

[5] Reasoning in AI refers to the informal mechanisms that large language models use to approximate the process of "making inferences, evaluating arguments, and drawing logical conclusions based on available information." See. Huang and Chang (2023), *Towards Reasoning in Large Language Models: A Survey*, May.

integration within the supply chain, particularly by global technology providers that offer both AI models and the infrastructure needed to train and deploy them (see Box 4 for further details of these developments). This vertical integration can enable efficiencies and innovation in the AI ecosystem, but also implies a high degree of control over key components, including computing power, data storage, and model access, which warrants monitoring to assess the implications for third-party dependencies and service provider concentration. These trends underscore the importance of continued close monitoring of AI advancements and their implications for financial stability, while also encouraging collaboration and exploring greater alignment in taxonomies and indicators to strengthen monitoring efforts.

In response to these developments, the South African G20 Presidency asked the FSB to prepare a report on how financial authorities can monitor AI adoption and assess related vulnerabilities. To fulfil this request, the FSB conducted a member survey on existing approaches to AI monitoring, complemented by interviews with authorities who have experience in this area. It also analysed public surveys, reports, and data sources, and engaged with external stakeholders, including FIs, academics, and AI service providers, through outreach meetings.

The rest of this report is structured as follows. Section 2 reviews monitoring approaches currently used by member jurisdictions. Section 3 lays out monitoring considerations and potential indicators for monitoring AI adoption and related vulnerabilities. Section 4 presents a case study on monitoring AI-related third-party dependencies and service provider concentration, elaborating on themes discussed in Sections 2 and 3. Section 5 concludes by summarising key monitoring issues and identifying high-level considerations to address gaps.

# 2. Monitoring approaches currently used by financial authorities

Jurisdictions, international organisations, and standard setting bodies[6] have carried out a range of studies and outreach initiatives concerning AI usage in the financial sector. In early 2025, the FSB fielded a survey to member authorities on the approaches they use to monitor AI adoption and related vulnerabilities (the “member survey”). Overall, 28 responses were received from authorities in 19 different jurisdictions and from one international organisation. Most respondents are responsible for supervisory functions within their jurisdiction, such as prudential bank supervision or market conduct oversight. This section examines AI monitoring approaches using findings from the member survey and other published studies.

## 2.1. Monitoring patterns

A large majority of survey respondents collect data on AI adoption in the financial system, but definitions of AI vary widely. The most common data collection approach is surveys targeting

[6] For example, the Basel Committee on Banking Supervision (BCBS) published a report on digitalisation of finance in 2024, which examines risks associated with GenAI. The International Association of Insurance Supervisors (IAIS) is gathering data on AI in insurance sector with the aim of publishing the conclusion as part of its Global Insurance Market Report. The International Organization of Securities Commissions (IOSCO) published a report that examines use cases, risks and challenges associated with AI in capital markets in March 2025. The BIS Committee on Payments and Market Infrastructures (CPMI) monitors, collects and exchanges information on key developments related to digital innovation including AI in payments and FMIs as part of its work programme and strategic priorities for 2025-27.

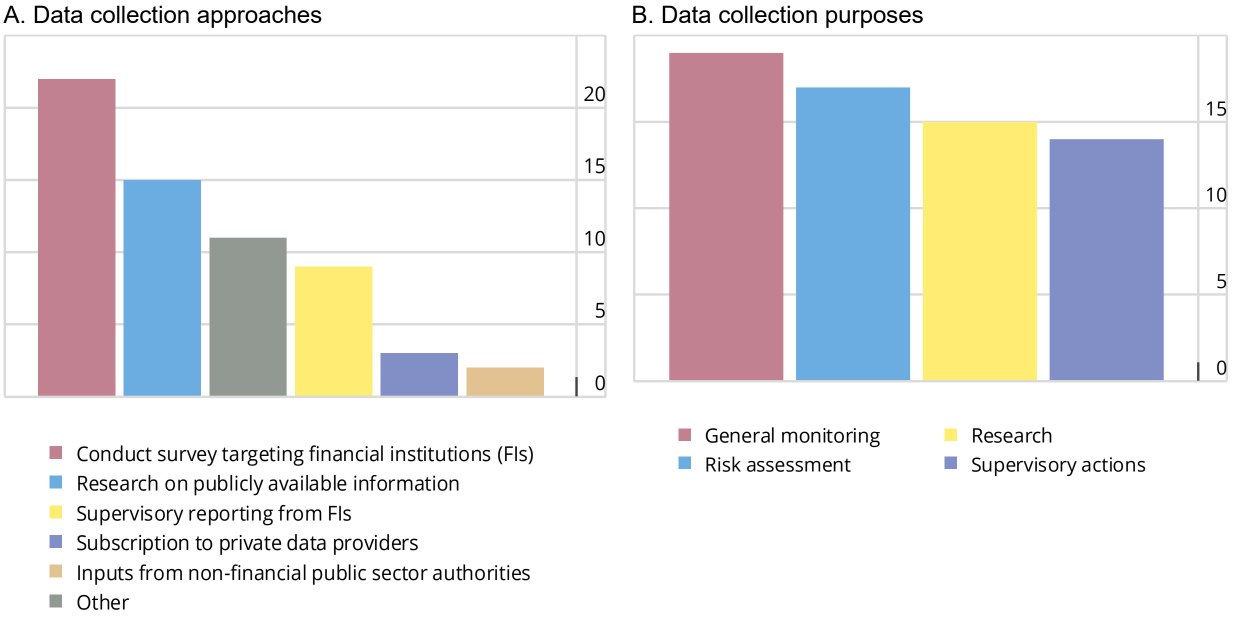
FIs' use of AI, followed by research using publicly available data. Many respondents also rely on supervisory reporting, while some subscribe to private data providers or receive indicators from other public authorities. Definitions of AI differ across jurisdictions: some authorities use the OECD or EU AI Act definitions,[7] others rely on jurisdiction-specific definitions, while a few have no specific definition. Graph 1 (left panel) illustrates the various approaches authorities use to gather data on AI adoption in the financial system.

Most supervisors collect AI-related data through surveys or reporting, with varying levels of participation, focus, and publication practices. Participation in most reporting initiatives is voluntary for firms, while the remainder require supervised firms to respond. Most supervisors collect data from institutions of all sizes, though some focus specifically on large institutions or adopt a mixed approach depending on the sector. AI-related supervisory reporting and surveys are typically conducted on an ad-hoc basis, although some authorities have established regular annual or biannual reporting. Just over half of the supervisors that collect AI-related data publish aggregate findings, while the remainder do not release any associated data. Graph 1 (right panel) shows that the reported data are used for a range of activities, including monitoring, risk assessment, research, and supervisory actions.

In addition to the data sources and collection strategies discussed above, respondents reported a variety of other monitoring approaches. These include tracking inventories of AI use cases in the financial sector, conducting AI-related requests for information, engaging in dialogue with industry through innovation hubs, collecting qualitative information from supervisory conversations with supervised firms, and analysing job postings and public disclosures.

**AI adoption data collection approaches and their purposes**

Count of responses **Graph 1**



Source: FSB. Note: results depicted in Graph 1 are not mutually exclusive.

[7] See OECD (2024), for a discussion on definitions. In the EU, the AI Act includes a regulatory definition of AI based on the OECD updated 2023 definition.

## 2.2. Vulnerabilities surveillance

The member survey reveals that monitoring specific AI-related financial sector vulnerabilities is more challenging than collecting data on adoption and use cases. Many respondents collect relevant data through broader supervisory initiatives, for example third-party risk management and operational incident monitoring (Table 1). While these initiatives are not specific to AI, many include information relevant to AI monitoring. In these broader initiatives it can be challenging to identify AI-specific vulnerabilities and events.[8] In addition, few respondents collect data on vulnerabilities associated with AI-related market correlations.

**Table 1: Approaches to monitoring AI-related vulnerabilities**

| Vulnerability | Monitoring approaches and related survey findings |
|---|---|
| **Third-party dependencies and service provider concentration** | • Many respondents include questions in surveys on the use of third-party AI applications and models.<br>• A few respondents pose survey questions about the materiality or criticality of AI applications, or about challenges associated with engaging third-party AI service providers.<br>• A few respondents noted AI-related third-party data collected as part of broader information collections on third-party risk management or indicated that they analyse publicly available data on AI supply chain concentration. |
| **Market correlations** | • A limited number of respondents have collection initiatives related to market correlations, such as monitoring patterns in AI-driven decision-making and signs of correlated market movements. Only a few respondents include questions in their surveys asking FIs to rank the potential systemic risks arising from herding behaviour and the use of common data and models relative to the other vulnerabilities from the use of AI in the financial sector.<br>• A few respondents reported collecting qualitative information from outreach initiatives with market contacts.<br>• Some respondents assess the potential for market correlations in conjunction with analysis of third-party concentration risk. |
| **Cyber** | • Many respondents report collecting data on cyber incidents in general, which include data on AI-related incidents.<br>• Several respondents include questions in surveys asking FIs about AI-related cyber vulnerabilities.<br>• Some respondents monitor publicly available data on AI cyber incidents. |
| **Model risk, data quality, and governance** | • Many respondents include questions in surveys asking FIs about AI-related governance mechanisms, model risk management challenges, and explainability approaches.<br>• Several respondents collect information on AI-related model risk management challenges through supervisory discussions, or by |

[8] In follow-up discussions, some authorities explained that they are reviewing the need for AI-specific data collection frameworks building on the existing technology neutral frameworks as AI technology and adoption in the financial system mature.

| Vulnerability | Monitoring approaches and related survey findings |
|---|---|
| | conducting a thematic review of AI-related model risk management practices at supervised firms.<br>• A limited number of respondents have issued guidance specific to AI model governance. |

## 2.3. Specific monitoring mechanisms

### *2.3.1. Supervisory monitoring*

AI-related supervisory monitoring enables authorities to enhance their knowledge of AI adoption across supervised firms. Over a third of respondents with supervisory authority reported that they have AI-related supervisory reporting in place. Several authorities without formal supervisory reporting approaches indicated that they have ongoing engagement with supervised firms on AI usage that facilitates monitoring. Some supervisors have ad-hoc monitoring arrangements, such as holding supervisory discussions and workshops to exchange views on selected use cases. While AI-related supervisory reporting can provide granular information about usage at supervised firms complementing information obtained from other monitoring approaches such as surveys, collecting data through this approach is less common among members as compared to surveys and publicly available information.

### *2.3.2. Surveys*

Surveys of AI usage at FIs often cover issues related to AI use cases and risks in detail, and their findings contribute to authorities' understanding of AI developments in finance. Fielding AI-related surveys targeting FIs is a widespread monitoring approach amongst survey respondents, with a substantive majority of respondents having carried out such surveys. A small majority of surveys are voluntary, and aggregate results are often published. Many surveys are fielded to one specific cohort of FIs, while other surveys are aimed at a variety of market participants. For example, the joint Bank of England (BoE) and Financial Conduct Authority (FCA) survey, and the Financial Services Agency of Japan (JFSA) survey, target a diverse range of FIs.[9] A similar effort in Italy is targeting all supervised financial market participants.[10] Other surveys focus on specific sectors, such as the IOSCO AI survey on capital markets.[11] While surveys provide valuable insights, direct engagement with FIs can help supervisors better understand the specific AI use cases associated vulnerabilities. Authorities report some challenges and limitations with surveys, including selection bias when participation is voluntary, and the costs involved.

[9] Bank of England and Financial Conduct Authority (2024), *Artificial intelligence in UK financial services - 2024*, November; Financial Services Agency of Japan (2025), *AI Discussion Paper Ver1.0: Preliminary Discussion Points for Promoting the Sound Utilization of AI in the Financial Sector*, March.

[10] The ongoing industry survey was conducted in H1 2025 by the OECD under the aegis of Banca d'Italia, the Commissione Nazionale per le Società e la Borsa (CONSOB), the Istituto per la Vigilanza sulle Assicurazioni (IVASS) and the Commissione di Vigilanza sui Fondi Pensione (COVIP) and supported by the European Commission.

[11] IOSCO (2025*), Artificial Intelligence In Capital Markets: Use Cases, Risks, and Challenges*, March.

### 2.3.3. Industry outreach

Several authorities use outreach initiatives to better understand AI usage, risk management, and specific areas of interest. Common outreach initiatives include roundtables, conferences, workshops, and working groups involving the financial sector and academia. Box 1 discusses examples from three authorities. Some respondents also engage with large technology firms, operate “Innovation Hubs”, or set up regulatory sandboxes. In several jurisdictions, outreach involves bilateral follow-ups to surveys to collect more detailed qualitative insights. Authorities also periodically issue AI-related requests for information from industry participants.

Outreach initiatives are valuable for gathering deeper insights into AI adoption but can present challenges. These initiatives enable data collection from diverse stakeholders (e.g. the US banking regulators’ 2021 Request for Information), provide a deeper understanding of AI applications and implementation challenges (e.g. BoE/FCA forum and JFSA AI forum) and support focused analysis of specific sectors (e.g. IMF Global Financial Stability Report (GFSR)). However, FIs may hesitate to disclose detailed information in public settings, such as roundtables or public comment requests. Furthermore, these initiatives can be costly, time intensive, and difficult to replicate over time. Their key advantage lies in their ability to complement other monitoring approaches.

**Box 1. Examples of AI-related industry outreach initiatives by financial authorities**

One approach involves soliciting public feedback on key issues related to AI in the financial sector. For example, in 2021, US federal banking agencies published a Request for Information (RFI) on FIs’ use of AI.[12] The RFI received around 100 public comment letters from diverse stakeholders, including FIs, technology firms, trade associations, consultants, and other interest groups. Respondents addressed a range of topics, such as AI use cases, benefits and risks, including those related to explainability, overfitting, third-party risk management and cybersecurity.

Another approach is facilitating dialogue through workshops, roundtables, conferences and other discussion forums. For example, the BoE and FCA launched the Artificial Intelligence Public-Private Forum (AIPPF) in 2020. Over the course of that year, the AIPPF hosted quarterly meetings and workshops with industry participants, academia, and public sector officials. The discussions focused on three areas: data, model risk, and governance. The initiative culminated in a final report summarising participants’ perspectives and potential mitigants.[13]

Finally, some authorities conduct structured confidential discussions with industry stakeholders, often complementing broader analytical work. For example, in its October 2024 Global Financial Stability Report, the IMF examined AI applications in capital markets.[14] Part of its analysis was informed by bilateral outreach sessions with capital markets participants, academics and AI vendors. These discussions combined quantitative and qualitative insights, informing key findings related to current and anticipated AI use cases in capital markets, associated risks and expected regulatory responses.

[12] Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency (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.

[13] Bank of England and Financial Conduct Authority (2022), *Artificial intelligence public-private forum: Final report*, February.

[14] IMF (2024), Advances in artificial intelligence: implications for capital market activities, in *Global Financial Stability Report*, Chapter 3, October.

### 2.3.4. *Publicly available and vendor data sources*

Publicly available data and vendor information are valuable tools for monitoring AI adoption in the financial sector, but they come with notable limitations (see Box 2 for illustrative examples). Publicly available data sources include business surveys, patent filings, public disclosures, job postings, and cyber incident monitoring (see Table 2). For example, business surveys, such as the US Census Bureau's *Business Trends and Outlook Survey* (the U.S. BTOS),[15] provide insights into firms' AI adoption. Textual analysis can also be used to glean information from public disclosures, job postings, and cyber monitoring systems. These data sources can be used to develop various AI adoption and usage indicators.

The motivation for using these data sources is multifaceted. First, they typically do not impose additional regulatory or data collection requirements on FIs. Second, certain indicators are refreshed more frequently than other collection methods. For example, the U.S. BTOS is published bi-weekly. Third, these sources are sometimes able to capture the diversity and scale of FIs, depending on their scope and coverage.

Nevertheless, indicators from publicly available data sources have their drawbacks. They often lack specificity about applications, such as operational efficiency, risk management, or the criticality of AI to a FI's core business. FIs relying on AI for certain types of business models or innovation strategies may be less inclined to disclose how they are employing AI. Including many small firms in the aggregate data can obscure the level of AI usage among larger institutions. Finally, the current focus of these indicators tends to be on adoption metrics, which may not align with the specific vulnerabilities highlighted in the 2024 FSB report. When using publicly available AI indicators, many of which are proxy indicators, it is prudent to analyse a comprehensive range of data sources and indicators collectively rather than relying on any single measure to assess AI adoption and related vulnerabilities in the financial sector.

**Table 2: Examples of publicly available and vendor data sources used for AI monitoring**

| Data sources | Description | Example sources and analyses |
|---|---|---|
| **Business surveys** | Representative business surveys carried out by statistical agencies that include questions about AI adoption. | The U.S. BTOS |
| **AI patents** | Trends in AI-related patent filings among groups of FIs or for specific types of financial activities. | IMF's analysis of AI-related patent applications in algorithmic trading using WIPO's Patentscope[16] |
| **Public disclosures** | Textual analysis of AI discussions in firms' investor disclosures, earnings call transcripts, and other public filings. | ESMA's AI-related term frequency analysis of regulatory and marketing documents from EU investment funds[17] |
| **Job postings** | AI-related job postings in the financial sector. | Indeed Hiring Lab; Lightcast; UMD-LinkUp AIMaps |

[15] U.S. Census Bureau (2025), *Business trends and outlook survey*, Washington: U.S. Census Bureau, accessed February.

[16] International Monetary Fund (IMF) (2024), *Global Financial Stability Report*, Chapter 3, October.

[17] Bagattini, Giulio and Federico Piazza (2025), Paris: European Securities and Markets Authority, February.

| Data sources | Description | Example sources and analyses |
|---|---|---|
| **Cyber monitoring** | AI-related cyber incidents. | OECD AI Incidents Monitor[18] |

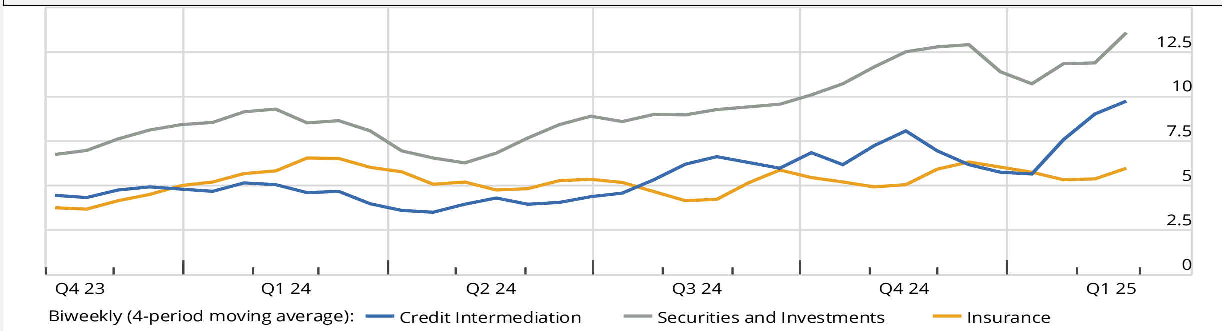
### Box 2. Examples of publicly available AI monitoring indicators

The U.S. BTOS includes two questions about AI adoption – whether a firm is currently using AI to produce goods and services, and whether they plan to do so in the next 6 months. Published biweekly, it is one of the highest frequency AI monitoring sources currently available. The survey shows that securities and investment firms tend to use AI more frequently than lending institutions and insurance companies, although lenders' AI usage has increased sharply this year (Graph A). The survey is relatively low-cost compared to bespoke data collection efforts and provides coverage across different types of institutions. However, coverage of the largest financial institutions in the survey is uneven.

**Use of AI by US FIs in "producing services"**

In per cent of firms

**Graph A**



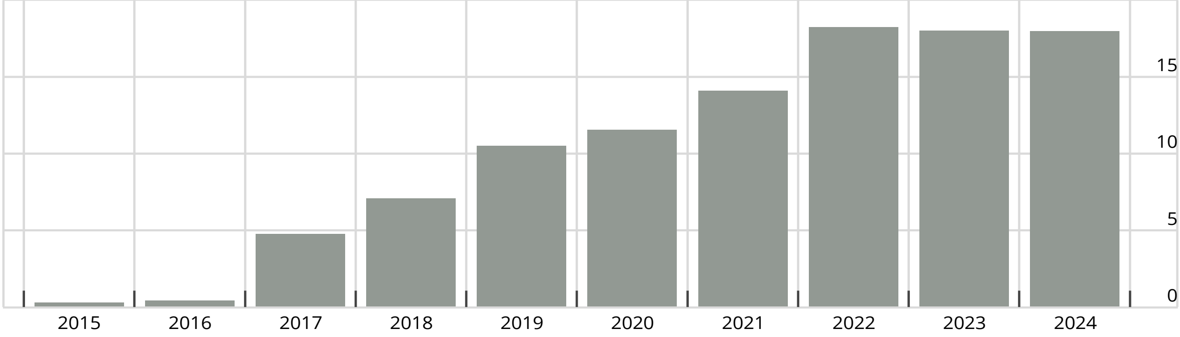
Source: The U.S. BTOS.

In its recent GFSR, the IMF analysed publicly available AI patent applications for algorithmic trading as an indicator of AI adoption in capital markets. It is also possible to examine trends in AI patents for cohorts of institutions. For example, over the past ten years, US global systemically important banks (G-SIBs) have filed more over 1,400 AI-related patent applications. Graph B plots AI patents as a share of total patents, a measure of AI innovation among these firms, which grew steadily for much of the past decade before levelling off over the last three years.

**AI related patent applications as a share of total applications (US G-SIBs)**

In per cent

**Graph B**



Source: World Intellectual Property Organisation, *PATENTSCOPE*.

[18] OECD (2025), OECD AI Incidents Monitor, accessed March.

# 3. Monitoring considerations and potential indicators

This section outlines considerations and potential indicators for monitoring AI adoption and related vulnerabilities. The intent of this section is to help financial authorities to evaluate and improve their data collection approaches in this area. Many of the indicators discussed in Section 3.3 could be collected directly from supervised firms through surveys, regulatory information collection, and outreach. However, other indicators may require more in-depth supervisory engagement with regulated firms. Authorities could pursue variations on these indicators and collection mechanisms depending on jurisdictional circumstances, such as the depth of AI adoption, market structure, and regulatory and supervisory frameworks.

## 3.1. Data collection design considerations

Several design features will help authorities to enhance the effectiveness and feasibility of data collection initiatives for monitoring AI adoption and vulnerabilities. Data sources will vary in terms of quality, consistency, and relevance to financial stability, and authorities will have differing capacities to collect data from supervised firms. The design considerations below can help authorities balance feasibility and ambition, while pursuing effective monitoring initiatives. National authorities are encouraged to pursue initiatives aligned with their monitoring goals, and incorporate the key considerations below where feasible, depending on the jurisdictional circumstances.

- **Relevance to vulnerabilities**: Collecting indicators that align with the AI-related financial sector vulnerabilities identified in the 2024 FSB report is essential for effective financial stability monitoring.

- **Representativeness**: Monitoring indicators that capture AI usage across different types of FIs in terms of financial activity, size, and regulatory status, among other factors, can provide a more holistic view of AI-related vulnerabilities than data limited to individual financial sub-sectors.

- **Standards and taxonomy alignment**: Although taxonomies for AI in the financial sector are still evolving and lack consistency, aligning, where possible, with definitions established by relevant authorities and standard setting bodies can help promote clarity, comparability and transparency.[19]

- **Timeliness**: Given the rapid developments in AI, data that are collected at regular intervals will be valuable for surveillance, as snapshots could quickly become outdated. At the same time, a flexible, forward-looking approach can help ensure that data collection initiatives adapt to the evolving environment.[20]

[19] For a discussion of AI-related taxonomy challenges, see Crisanto et al. (2024), *Regulating AI in the financial sector: recent developments and main challenges*, BIS: FSI Insights on Policy Implementation, No 63, December; and OECD (2024), *Regulatory approaches to Artificial Intelligence in finance*, September.

[20] For example, the Financial Policy Committee of the BoE pointed out that an approach to monitoring AI risks will need to be flexible and forward-looking. See FPC (2025), *Financial Stability in Focus: Artificial intelligence in the financial system*, April.

- **Burden sensitivity**: Proportional, risk-based monitoring initiatives can help ensure efficiency and effectiveness while lessening the regulatory burden and cost inherent in data collection. Authorities could also leverage existing reporting frameworks (e.g. operational risk or model risk management reporting) where possible. Encouraging information sharing between authorities can reduce duplicative efforts and improve representativeness.

## 3.2. Challenges and potential mitigation strategies

Respondents to the member survey highlighted several key challenges in collecting data and information on AI adoption in the financial system. These challenges fall into three main categories: definitions and comparability, cost and scope of monitoring, and assessing the criticality of AI services.

- **Definitions and comparability**: Rapid technological advancements and evolving taxonomies make it challenging to maintain consistent data collection frameworks over time. Respondents highlighted that this is made difficult by the absence of standardised definitions, metrics and reporting frameworks, leading to inconsistent reporting practices. For example, some firms classify models obtained from third-party providers and subsequently modified in-house as "third-party" models, while others consider such models to be "internally developed".

- **Cost and scope of monitoring**: Data collection is resource-intensive for both supervised firms and supervisory authorities. While proportional, risk-based initiatives (as discussed in Section 3.1) can help reduce the regulatory burden, respondents noted challenges such as selection bias in voluntary surveys and difficulty monitoring third-party AI providers that are outside the scope of financial sector regulation or supervision. Follow-up discussions with firms are often required to contextualise the collected data. Similarly, authorities have faced challenges ensuring regular data collection. This could be exacerbated by resource and capacity constraints at financial authorities. The survey results show that less than half of respondents collect monitoring data annually, and no authorities collect data more frequently.

- **Assessing criticality:** Assessing the criticality of AI services is challenging, as it requires a deep understanding of how AI interacts with an FIs' operations, and the sector-wide dependencies that exist on certain providers, models, and training data sets. Surveys alone may be insufficient for this purpose. More detailed information collection approaches may be necessary to address these gaps (see Section 4 for further details).

In addition to the key challenges cited by authorities, the survey results revealed that it is difficult to map existing indicators to specific vulnerabilities (as discussed in section 2.2). Follow-up interviews with member authorities revealed challenges in identifying the AI-specific aspects of certain types of vulnerabilities, such as those related to market correlations. Some authorities also noted the tension between maintaining a technology-neutral approach and assessing AI-specific vulnerabilities. A technology-neutral approach promotes consistency and adaptability across various technologies, but authorities in some jurisdictions may find it challenging to comprehensively assess risks that are heightened with AI, such as explainability challenges or a lack of transparency in pre-trained models. Despite these challenges, the authorities that were interviewed indicated a preference to maintain technology-neutral approaches and plan to rely on existing policy frameworks unless the development of AI-specific frameworks becomes necessary. These authorities expressed confidence in balancing the need to monitor AI-related vulnerabilities while preserving the broader applicability and coherence of regulatory frameworks.

Respondents proposed a number of approaches to improve their data collection initiatives. Several respondents suggested that international bodies could facilitate the development of more comparable taxonomies and indicators that could aid transparency, comparability, and consistency in data collection. Members also recommended simplifying surveys to a few high-value questions. This could reduce collection burdens, improve response rates, and make regular data collections more feasible.[21] Further, some respondents recommended sharing data across sectoral regulators as this could increase the representativeness of the data samples. There were also suggestions to utilise multiple indicators to monitor AI adoption and combining quantitative survey responses with qualitative follow-up interviews to enhance monitoring efforts further. While not specifically discussed in the survey, ongoing global regulatory initiatives could also facilitate AI monitoring and help reduce duplicative information collection initiatives.[22]

Most respondents plan to expand their AI-related data collection initiatives, focusing on standardisation, industry engagement, and sustainable monitoring approaches. These include evaluating their existing survey data, introducing standardised reporting requirements, and potentially issuing supervisory guidelines for AI in finance. Many authorities also plan to deepen their engagement with the industry to better understand the evolving AI landscape and its implications for the financial stability. Key focus areas for authorities include third-party relationships, AI use in algorithmic trading, and the intensity of AI use in FIs. Embedding questions within existing monitoring initiatives may offer a more efficient alternative to launching new standalone surveys.

## 3.3. Monitoring indicators

Monitoring AI adoption and assessing related vulnerabilities requires a comprehensive approach that draws on a diverse set of indicators from multiple sources. To help authorities address the challenges discussed above and make progress in monitoring AI adoption and the vulnerabilities identified in the 2024 FSB report, this section identifies a series of potential monitoring indicators. Section 3.3.1 presents potential indicators to help authorities to monitor AI adoption, while Sections 3.3.2-3.3.6 present examples of indicators for specific vulnerabilities. Some indicators seek to directly assess specific vulnerabilities (direct indicators), while others serve as proxies by offering indirect insights into vulnerabilities (proxy indicators). As outlined in the previous section, authorities are encouraged to adopt a risk-based and proportionate approach to prioritising indicators most relevant for monitoring AI adoption and the related vulnerabilities.

[21] One authority that achieved a very high response rate to a voluntary survey credited the simplicity of the questions and the ease of completing the survey for respondents that did not have much to report.

[22] Examples include BCBS (2024), *Consultative Document Principles for the sound management of third-party risk*, July; and IAIS (2025), *Application Paper on the supervision of artificial intelligence*, July.

### *3.3.1. AI adoption*

The systemic relevance of AI in the financial sector depends on the depth of AI adoption and the use cases that AI supports. Authorities can use a combination of direct and proxy indicators to assess the extent of AI adoption and its implications.

Direct indicators provide granular insights into AI adoption. Examples include:

- **Inventories of AI use cases in the financial sector with breakdowns along relevant dimensions:** These inventories provide a detailed overview of how AI is applied across three key dimensions: (i) financial activity (e.g. trading, lending, insurance, payments), (ii) types of AI (e.g. generative, agentic, others),[23] and (iii) levels of materiality (e.g. core business lines, critical operations, or low risk internal processes).

- **Share of institutions that use AI by type of use cases, AI models and size of FIs:** Authorities could track the proportion of FIs adopting AI, segmented by their size and type of use cases and AI models for identifying adoption trends over time.

- **Qualitative data on AI adoption patterns by cohorts of institutions:** Derived from industry outreach and public information (e.g. annual reports, press releases). Qualitative indicators can supplement quantitative metrics and help identify key trends, such as the specific use cases being prioritised by FIs, common challenges faced (e.g. regulatory uncertainty or technical expertise gaps) and deployment approaches (e.g. partnerships with AI vendors or in-house development).

Where direct data collection initiatives are challenging to implement, proxy indicators can serve as useful alternatives or supplements. Examples include:

- **AI-related patent applications:** The number of AI-related patents filed by FIs.

- **Trends in AI-related roles within FIs:** Aggregated by third-party data providers or researchers, this indicator reflects the demand for AI-related skills and roles within the financial sector, providing insights into workforce transformation driven by AI adoption.

- **Technology or research and development (R&D) spending as proxy for AI investment:** Overall technology and R&D spending reported in FIs' public filings can serve as a proxy for assessing the strategic importance of AI. This can be complemented by textual analysis of AI-related discussions in investor disclosures, earnings call transcripts, and other public documents such as research papers published by FIs to infer the level of AI focus and investment.

Section 2.3.4 discusses more specific examples of, and trade-offs inherent in, these types of publicly available indirect indicators.

[23] Agentic AI, a less formalised concept, describes systems designed to autonomously perform complex tasks over extended periods, often making decisions and taking actions with limited human oversight. While distinct, generative AI is often integrated into agentic AI systems to enhance their ability to generate content, simulate scenarios, or communicate dynamically. See Acharya et al. (2025), *Agentic AI: Autonomous Intelligence for Complex Goals–A Comprehensive Survey*, IEEE Access, 13: 18912 - 18936.

### *3.3.2. Third-party dependencies and service provider concentration*

Monitoring AI-related third-party dependencies and service provider concentration requires indicators that measure the extent to which FIs use AI services provided by third parties, as well as the criticality and substitutability of those services. Section 4 presents a more in-depth case study on key considerations for monitoring this vulnerability and approaches authorities have used to date. Representative examples of indicators are presented below. Most of these would need to be collected directly from FIs or paired with regulatory financial data, but some can be derived from public sources.

- **Share of FIs' AI applications made available by third parties**: Provides a global view of the extent of AI-related third-party dependencies in the financial sector.

- **Notifications to authorities by FIs of material cyber and operational incidents affecting services provided by third-party AI service providers**: Enables monitoring of a primary channel through which this vulnerability can translate into operational losses for FIs.

- **Registers of critical AI services and service providers based on data and information collected from supervised FIs**: Helps assess the criticality of AI services in the financial sector and aspects of the AI supply chain that could amplify vulnerabilities.

- **Number of critical AI services supported by a single or closely connected AI service providers**: Helps measure and monitor AI service provider concentration risk.

- **Number of global or domestic systemically important FIs for which third-party AI services support critical operations:** Contributes to assessing the systemic relevance of third-party dependencies and service provider concentration.

- **Relative cost and performance of widely used AI services:** Helps measure the substitutability of AI services; would generally need to be derived through public sources, such as large language model (LLM) leaderboards, service provider websites, and publications about model performance.[24]

### *3.3.3. Market correlations*

Monitoring AI-driven market correlations requires indicators that estimate the effect of AI adoption on market dynamics, including herding behaviour, liquidity crunches, and pro-cyclicality. Attributing and monitoring AI-driven market correlations is necessary to identify related vulnerabilities, as similar AI models and data sources may have the potential to amplify systemic risks like herding,[25] liquidity crunches, and pro-cyclicality, however it has been challenging for authorities to attribute and monitor correlations thus far (see Section 2.2). The

[24] LLM leaderboards are rich sources of information about the relative cost and performance of leading LLMs. For examples of leaderboards, see: LMArena, *Leaderboard* and Artificial Analysis, *LLM Leaderboard* Service provider websites often include information on pricing, along with documentation that outlines how their LLMs perform, including key capabilities, limitations, and intended use cases.

[25] ECB (2024), *The rise of artificial intelligence: benefits and risks for financial stability*, May.

challenges involved were noted in the FSB's 2017 report on AI, [26] which highlighted the difficulty of monitoring such risks, especially given the opacity and unpredictability of certain AI models.[27]

Direct indicators, such as a measure of interactions between AI models or stress testing results, are not currently available, so the indicators listed below are proxies. There is still little empirical evidence that AI-driven market correlations affect market outcomes; however, as highlighted in the 2024 FSB report on AI, these dynamics may evolve alongside the rapid pace of AI innovation. With these considerations in mind, types of indicators that can help monitor this vulnerability include:

- **Number of FIs using each of the widely used pre-trained model, their features, and/or training data sources**: [28] Third-party dependencies and service provider concentration may contribute to market correlation vulnerabilities. For example, reliance on a limited number of pre-trained models with similar features (e.g. model class, structural design, time horizon, or objective function) and/or training data sources may drive similar behaviours across institutions, amplifying correlations in financial markets.[29] This indicator could track the concentration of widely used models and their associated features, helping to identify potentially correlated behaviours among FIs.

- **Analytical measures of association between AI adoption in specific use cases and asset price volatility or correlations in capital market segments:** Attributing market correlations to AI adoption could involve analytical methods such as regression analysis, event studies, machine learning models, and network analysis to examine large datasets, including both structured data (e.g. trade volumes) and unstructured data (e.g. text from financial news or social media). These tasks are complex, and authorities may benefit from close collaboration with the academic research community to develop meaningful indicators.[30] While these methods are well-established, their application in this context is not and may require caution due to limited transparency in AI adoption, difficulties in establishing causality, and the risk of model mis-specification under shifting market regimes.[31]

- **Information around the level of autonomy of AI models in key markets:** Authorities could explore ways to enhance their knowledge of market practices and developments around AI-automated trading strategies, credit decisions and asset allocation in key markets. A higher level of autonomy may increase the risk of AI driven market

[26] IOSCO also pointed out the challenges in monitoring AI related market correlations due to lack of sufficient data. See IOSCO (2025), March.

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

[28] External suppliers of datasets are also used by financial institutions to power AI inferences, ranging from macroeconomic indicators and market sentiment to alternative data like satellite imagery or social media trends.

[29] As noted in the 2024 FSB report on AI, "the homogenisation in training data and model architecture can lead to correlated outputs, which could amplify market stress and exacerbate liquidity crunches."; see FSB (2024).

[30] Time-series models, for instance, are well-suited to capturing structural changes in volatility patterns over time, while event studies allow for the identification of market reactions to discrete AI-related developments, such as the introduction of a new trading algorithm or regulatory interventions. Network analysis could also provide insights into systemic risks if dependencies on shared AI models or datasets are identified. There are some early examples of potentially useful methods academics are pursuing to measure activity in this area. For example, a recent working paper found robust associations between ChatGPT outages and various trading market dynamics, such as volume, return variance, and bid-ask spreads. See: Cheng, Qiang, Pengkai Lin, and Yue Zhao (2024), *Does Generative AI Facilitate Investor Trading? Evidence from ChatGPT Outages*, Singapore Management University School of Accountancy, Research Paper No. 2025-186, June.

[31] IMF (2024), *Global Financial Stability Report, Chapter 3*, October.

correlations due to a lack of human intervention. In this respect, the risk management techniques of the firms are expected to include an assessment of the specific risk of the application. Authorities could encourage firms to share sufficient information on the assessment made to support effective oversight and systemic risk monitoring. Collaborative stakeholder engagement can help achieve this balance.

### *3.3.4. Cyber*

Monitoring AI-related cyber vulnerabilities involves assessing both external threats, and FIs' cyber defences. As discussed in the 2024 report, AI can augment malicious actors' cyber capabilities. AI adoption by FIs can also increase attack opportunities due to intense data usage and novel ways of interacting with external systems. At the same time, authorities and FIs can leverage AI to enhance cyber defence systems. While authorities have made progress in monitoring AI-related cyber vulnerabilities, challenges remain. Many jurisdictions already collect data on general cyber incidents, which often include AI-related cases. To enhance monitoring, authorities could leverage existing supervisory frameworks, such as operational risk reporting and third-party risk management, to integrate AI-specific indicators into their processes. The FSB's FIRE framework (Format for Incident Reporting Exchange) could also play a critical role by providing a standardised approach for reporting operational and cyber incidents, including those related to AI.[32] The following indicators could be used to track AI-specific cyber vulnerabilities by assessing external and internal threats, as well as usage to enhance defence systems:

- **Number of AI-related cyber-attacks targeting the financial sector:** Helps authorities monitor external sources of cyber vulnerabilities related to AI. Attacks could be categorised by type, such as data and model poisoning, prompt injection, and other emerging threat patterns facilitated by AI.[33]

- **Number of internal cyber incidents related to AI:** Helps authorities record internal sources of cyber vulnerabilities at FIs related to AI. These data could be collected from supervisory operational risk monitoring initiatives. Relevant incident types could include unauthorised leaking of sensitive proprietary data to external AI tools, model configuration errors, and the identification of AI application security vulnerabilities.

- **Number of third-party AI incidents**: AI-related cyber incidents affecting FIs' third-party service providers, such as cloud platforms and model developers. This indicator can help authorities understand FIs' indirect exposure to AI-related cyber vulnerabilities and single point of failure risks that could affect multiple FIs simultaneously.

- **AI use cases for cyber defence:** Registers of AI-related cyber defence use cases can help authorities and FIs learn about and adopt such systems, where appropriate, to augment cybersecurity. Examples of use cases include AI-driven anomaly detection

[32] By leveraging the FSB's Format for Incident Reporting exchange, authorities can ensure consistency in incident reporting, improve cross-border coordination, and enhance their ability to identify systemic vulnerabilities. FSB (2025), *Format for Incident Reporting Exchange (FIRE)*, April.

[33] Data and model poisoning refer to incidents in which attackers manipulate training data or model weights. Prompt injection occurs when attackers manipulate GenAI tools or LLMs to extract confidential information. See IBM (2024), December.

systems, which improve real-time identification of unusual activity or potential attacks, and incident response automation tools, which leverage AI to streamline and accelerate responses to cyber incidents. Supervisory reviews and surveys could provide insights into the adoption of these measures.

### *3.3.5. Model risk, data quality, and governance*

Monitoring AI-related model risk, data quality, and governance vulnerabilities involves developing more holistic, system-wide surveillance metrics for issues that many micro-prudential authorities already assess at the institution-specific level. As explained in the 2024 FSB report, wider AI uptake can increase model risk in the financial system due to limited explainability of some AI approaches and a lack of transparency in training data sources, among other factors. As AI models become more complex, financial authorities face increasing difficulties in understanding them. Additionally, it can be more challenging to assess the quality and accuracy of LLM outputs than quantitative forecasts made by machine learning models, especially given new forms of model inaccuracies, notably LLM hallucinations.[34] The accessibility and utility of GenAI services may also incentivise FIs to adopt these technologies without requisite governance frameworks. As highlighted in the 2024 FSB report, these factors contribute to misaligned AI systems, which represent a key governance-related vulnerability. Box 3 provides further detail on misaligned systems and their implications for financial stability. Micro-prudential supervisors in many jurisdictions evaluate these issues at the institution level through supervisory activities such as model risk management exams.[35] Expanding the focus to include vulnerabilities across institutions and sectors could strengthen global efforts to monitor financial stability.

Indicators for Monitoring Model Risk, Data Quality and Governance:

- **Share of AI models in FIs' model inventories**: Collecting data across supervised institutions that measure the overall share of AI models in model inventories provides information on the scale of adoption for modelling purposes. Distinguishing high-risk AI use cases from less risky applications may also be useful.

- **Trends in supervisory findings related to AI model risk management and governance**: Developing aggregate metrics on the number of supervisory findings related to AI model risk management and governance can help authorities monitor the evolution of vulnerabilities in this area. Ideally, these metrics could be broken out by the source of deficiency (e.g. explainability, model validation, outcomes analysis, data governance).

- **Degree of automated decision-making in AI systems:** Monitoring the extent to which FIs use human-in-the-loop interactions with AI models and rely on automated decision-making can help authorities assess risks related to model risks, data quality and governance. Authorities could also engage with regulated FIs to understand use cases involving automated decision-making or the adoption of agentic AI.

[34] A hallucination occurs when an LLM provides a seemingly confident but inaccurate response to user inputs.

[35] In some cases, such as Singapore's AI Verify Foundation, government authorities (beyond financial sector authorities) involve private sector efforts to enhance AI testing tools and practices. See. AI Verify Foundation

**Box 3. Misaligned AI systems**

The 2024 FSB report identified “misaligned” AI systems as another vulnerability. Misalignment refers to the divergence between an AI system’s objectives, outputs, or decision-making processes and the intended standards or principles set by its developers or users, that could produce outputs violating established rules, creating compliance risks, or leading to unethical outcomes. For example, limited explainability in AI models, a lack of transparency in training data sources and inaccuracies like LLM hallucinations can contribute to misaligned systems. Given the novelty and complexity of this vulnerability, practices to identify and address misaligned AI system are not well developed and thus it is hard to identify specific indicators that help authorities to assess the related vulnerability as of now. Nonetheless, assessing model inventory at FIs and FIs risk management approaches could help authorities to monitor the vulnerability, in particular the share of critical AI systems that are not calibrated to operate within legal, regulatory, and ethical boundaries.

### *3.3.6. AI driven financial fraud and disinformation*

AI driven financial fraud and disinformation could impact financial stability by eroding trust, amplifying volatility and potentially triggering events such as flash crashes or bank runs (as discussed in the 2024 FSB report). While these threats primarily stem from external actors, their potential impact underscores the importance of monitoring. Authorities could consider several types of indicators.

- **AI-driven financial fraud:**[36] This includes tracking the number of fraud cases involving GenAI, such as the use of deepfakes, synthetic identities, or fraudulent claims. At the same time, authorities should explore ways to qualitatively evaluate how FIs are prepared, including through leveraging AI tools for fraud detection and prevention, such as systems designed to identify anomalies, flag suspicious transactions, or enhance investigative capabilities.

- **Disinformation campaigns:**[37] This involves assessing the prevalence of AI-generated disinformation that could disrupt financial markets and evaluating its potential impact on market stability. This includes tracking instances where AI-generated content, such as false news or manipulated media, spreads misinformation that influences investor behaviour or market sentiment.

- **Customer complaints reports linked to AI fraud and disinformation:** Customer complaints reports could serve as the first level signal of increase in AI related fraud and disinformation campaigns. Authorities could analyse such reports to detect commonalities and trends in fraud and disinformation cases.

[36] Since AI-driven frauds specifically target financial deception or abuse of trust, they differ from broader AI-enabled cyber threats (e.g. to digital infrastructure, data integrity and system resilience).

[37] Unlike financial fraud, which typically targets individual entities, AI-driven disinformation campaigns aim at manipulating public perception and compromise information integrity through digital channels. Disinformation campaigns could amplify volatility, disrupt confidents in FIs and, under certain conditions, trigger flash crashes, bank runs, or other destabilising events.

# 4. Case study – monitoring AI-related third-party dependencies and service provider concentration related to GenAI

The 2024 report identified several developments that could amplify vulnerabilities stemming from AI-related third-party dependencies and service provider concentration in the financial sector. These developments include the emergence of GenAI and LLMs, which have created a number of novel use cases that a wide range of financial institutions are exploring and integrating into their business activity. The 2024 report noted that financial institutions appear to be taking a cautious approach to adopting GenAI, with apparently limited use for critical functions and critical operations so far. However, interest among FIs in the application of GenAI remains high, and the technology's accessibility could facilitate rapid integration into financial services. While accessibility is a driver of adoption, the 2024 report also highlighted that it could amplify vulnerabilities, such as reliance on third-party providers or concentration risks. This case study discusses monitoring of some of the vulnerabilities that could be potentially amplified by greater adoption of GenAI into core financial services activities.

GenAI uptake in finance is often through pre-trained models that rely on specialised hardware and cloud services for AI development. FIs would face significant constraints in cost and talent acquisition if they were to try and develop these models internally—so much so that the choice is often between using these models or no use of GenAI at all. However, the continued and expanding use of GenAI may create greater third-party dependencies among FIs on the service providers for these leading GenAI models. Additionally, concentration exists in key aspects of the GenAI supply chain, such as the hardware, cloud, training data, and model markets. Third-party services, including reliance on well-resourced third-party providers, can bring multiple benefits to financial institutions, including flexibility, innovation, and improved cyber and operational resilience. However, if not properly managed, the interaction of third-party dependencies and service provider concentration can reduce FIs' ability to mitigate the impact arising from disruptions affecting third- and nth-party[38] service providers, such as operational impairments or supply chain disruptions. The systemic relevance of this vulnerability depends on the extent of GenAI adoption in finance and the criticality and substitutability of GenAI services for FIs. Also, dependencies and concentration appear to be more prevalent in GenAI than other types of AI and machine learning to date.

Authorities have more experience in monitoring third-party dependencies and service provider concentration than other AI-related vulnerabilities, but challenges remain. While financial authorities have made some progress in monitoring AI adoption across the financial sector, it has been more challenging to monitor and assess the specific vulnerabilities identified in the 2024 report (see section 2). Among the vulnerabilities, the member survey revealed that authorities have made the most progress in monitoring AI-related third-party dependencies and service provider concentration, often due to existing frameworks. This section draws on FSB policy work and authorities' experiences to present a case study on monitoring and assessing third-party dependencies and service provider concentration. As background, section 4.1

[38] 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 (2023), *Enhancing Third-Party Risk Management and Oversight*, December.

provides a short overview of the AI supply chain and identifies developments since the 2024. Section 4.2 takes a deeper dive on how authorities are monitoring this important vulnerability. Finally, section 4.3 leverages the FSB's third-party risk management toolkit ("FSB toolkit") to present detailed monitoring considerations in this area.[39]

## 4.1 Overview of the GenAI supply chain

The structure and diversification of the GenAI supply chain are important determinants of the extent to which third-party dependencies and service provider concentration may interact to amplify operational vulnerabilities for FIs that use GenAI. The GenAI supply chain comprises five main layers:[40,41]

- **Hardware**: Computing chips necessary for training and using many AI models, including graphics processing units (GPUs) and other AI-specialised chips. The market for specialised computing chips is currently the most concentrated aspect of the AI supply chain,[42] though Box 4 discusses some developments that could increase competition in this area.

- **Computing infrastructure:** Primarily revolves around cloud services, which are crucial for the development and distribution of state-of-the-art GenAI applications. This layer is also significantly concentrated among a few global technology providers,[43] which benefit from substantial prior investments (leading to high barriers to entry), significant switching costs for users, and their ability to offer vertically integrated solutions.

- **Training data:** Large datasets require significant resources to aggregate and manage. While some data is publicly available, much of it is proprietary or sourced from third-party aggregators. Entities with established data pipelines and extensive user bases benefit from economies of scale and network effects – the more data they have, the better their services become. This attracts more users and generates even more data, creating a data-network-activities (DNA) loop.[44] Over time, this loop reinforces control over access to high-quality, relevant data due to their capacity for large-scale collection and storage.

- **Pre-trained foundation models:** Large-scale AI models, such as LLMs, that are trained and disseminated by third parties, such as AI firms.[45] The market for pre-trained models demonstrates tendencies towards concentration as the development of large-

[39] FSB (2023), *Enhancing Third-Party Risk Management and Oversight*, December.

[40] This section is based on the supply chain framework described by Gambacorta and Shreeti (2025), *The AI supply chain* BIS Papers, No. 154, March.

[41] In some cases, this report refers to specific firms providing AI-related services as examples. These examples are not exhaustive and do not constitute an endorsement by the FSB or its members for any firm, product, or service.

[42] For example, key players in this market include NVIDIA, AMD, Intel, and TSMC.

[43] Key players in this segment include AWS, Alibaba, Google Cloud and Microsoft Azure.

[44] Shin (2019), *Big tech in finance: opportunities and risks*, Speech to the BIS Annual General Meeting, June.

[45] For example, firms such as Alibaba, Alphabet, Amazon, Baidu, Meta, Microsoft, and Tencent, and as well as AI start-ups such as Anthropic, DeepSeek, Mistral, Monica, OpenAI and xAI, among others.

scale, general-purpose foundation models is characterised by high barriers to entry due to significant upfront investment in research, computational infrastructure, and extensive high-quality datasets. Providers in this space often benefit from a first-mover advantage in terms of accumulated resources and brand recognition. However, the emergence of lighter, open-weight models offers the potential to challenge this dominant position by lowering some barriers to entry and increasing deployment flexibility (see Box 4).

- **User-facing applications:** The layer that governs how end-users interact with AI models for specific use cases. The market for AI applications exhibits heterogeneous degrees of concentration depending on the specific application domain. For instance, a few dominant platforms might control the market for AI-driven customer relationship management tools in finance. This concentration often arises from strong network effects, data advantages, reputational advantages, and the benefits of integrating AI functionalities into existing software ecosystems.

Vulnerabilities related to the GenAI supply chain will be influenced by the nature of AI adoption among FIs, the level of concentration among AI service providers, and the trend toward vertical integration within the supply chain. If FIs increasingly deploy AI in core business lines and critical operations, then operational disruptions could have more impact if reliance is placed on few providers. High levels of concentration in the AI supply chain could limit substitutability given the small number of alternative service providers in the market and thus amplify vulnerabilities. Moreover, challenges could emerge if FIs rely on too many providers of critical and non-critical services, making their infrastructure more complex and difficult to effectively manage.

The technical features of AI solutions can significantly shape the relevance of different layers within the AI supply chain. For example, access to GenAI systems in finance is often provided through online interfaces or tools built on cloud infrastructure,[46] potentially making the underlying cloud services a critical part of how these systems operate. In this context, proprietary, or 'closed,' models may confine users to the vendor's infrastructure, whether directly or through cloud-based LLM platforms. Similarly, the recent focus by technology firms on developing agentic AI services, which are designed to be integrated with a wider range of business tools, could increase reliance on firms developing these systems. Conversely, open-weight models (see Box 4) can reduce dependence on specific providers, as they can be sourced from open repositories and stored locally with on-premises infrastructure. Small language models stand out in this regard, demanding substantially less data and computing power for training, tuning, and, crucially, deployment (inference), when compared to their larger counterparts, LLMs.

[46] Bank of England and Financial Conduct Authority (2024), *Artificial intelligence in UK financial services - 2024*, November; Financial Services Agency of Japan (2025), *AI Discussion Paper Ver1.0: Preliminary Discussion Points for Promoting the Sound Utilization of AI in the Financial Sector*, March.

### Box 4. Recent developments in the GenAI supply chain

Since the 2024 FSB report, there have been several AI supply chain developments related to pre-trained models, vertical integration, and the hardware market that have the potential to affect the relevance of third-party dependencies and service provider concentration. Monitoring developments in the AI supply chain is important for assessing vulnerabilities in this area.

**Models**

The release of highly performant, lower-cost, open-weight AI models, such as DeepSeek's R1 model[47] could potentially challenge the current development paradigm, which hinges on massive investments and heavy computation. These alternatives may lower the barriers to entry for organisations seeking advanced AI capabilities and offer diverse deployment options mitigating concentration risks.

Similarly, advancements in open-weight models, whose internal parameters are publicly available for review and customisation, could accelerate the trend towards provision of increasingly specialised AI solutions and reduce vendor lock-in. Improved performance and wider availability of specialised models could, in turn, help organisations diversify their AI infrastructure and lessen dependence on proprietary, closed solutions from a limited number of service providers. Despite the availability of competitive open-weight options, proprietary models are more widely performant and widely used.[48]

Finally, most leading AI firms are developing and emphasising multi-step "reasoning" models, which have proven to perform a variety of complex tasks well. These models essentially work by breaking problems down into sub-parts to be solved in a structured manner. In practice, this means that they use more inference computing power and are thus higher in marginal cost than their predecessors. Because they typically improve on base LLMs, reasoning models do not require as much up-front investment to train. Economic theory suggests that lower fixed cost industries attract competition. While the trend toward reasoning models might encourage new providers to enter this specialised segment, the inherent complexity of such models and higher marginal costs (for inference) could still lead to concentration among those providers with the technical skills and infrastructure to refine and support them at scale.

**Vertical integration**

Global technology providers are active across the AI supply chain and are increasingly integrating both upstream and downstream, combining services across hardware, cloud infrastructure and AI models. Providers bundle services and may impose conditions or pricing structures that discourage the use of non-affiliated technologies. Some cloud service providers are expanding into hardware and data markets, as well as securing dedicated energy sources to support their operations.[49, 50] Additionally, several providers now offer large or small language models optimised for their own infrastructure, which can deliver high performance, competitive pricing and faster deployment. While vertical integration offers users convenient and high-performing AI solutions, it reinforces dependencies on single providers, potentially increasing switching costs and limiting interoperability with alternative infrastructures or models. This trend could exacerbate service provider concentration.

**Hardware**

There are some early but still modest indications of increasing competition in the markets for GPUs and other specialised AI chips.[51] It is possible that the hardware market could mature to offer viable alternatives to the currently dominant players. Diversification of chip suppliers would reduce a critical point of dependency. However, the development and scaling of these alternative providers remain uncertain and may take time.

## 4.2 Current monitoring approaches

A number of authorities are monitoring AI-related third-party relationships, but less progress has been made in assessing criticality and GenAI service provider concentration. Among the supervisory authority respondents to the member survey, many reported specific monitoring approaches for AI-related third-party dependencies. Some other authorities also collect information on relationships with AI service providers through broader data collection initiatives related to third-party risk management. A few respondents plan to include questions about this vulnerability in a future survey. Most of these initiatives focus broadly on AI-related third-party relationships. A few respondents appear to be focused on assessing the criticality of AI services. Several respondents evaluate concentration risk based on the service providers that FIs use most often. Another few report measures to monitor the market for AI services, including exploring sources of concentration in the AI supply chain. However, there is not much evidence that authorities are evaluating the substitutability of AI services in depth.

Most monitoring initiatives in this area are carried out through surveys. The most common way that authorities are monitoring this vulnerability is by posing survey questions to FIs about the number of AI applications they are using, and the extent to which the applications are developed by third parties. Another common approach is to ask FIs about risk management approaches or challenges related to AI service providers. Surveys generally do not involve AI service providers themselves. Box 5 profiles some findings from publicly available surveys that include components focusing on this vulnerability. While assessing the criticality of AI services appears rare at this point, a few authorities report promising monitoring approaches in this regard. For example, some authorities ask FIs to report the number of critical AI applications, the extent to which the critical applications are developed externally, the top service providers for such application, and to rate the materiality of AI use cases. These measurement approaches tend to rely on institutions' own assessments of criticality.

### Box 5. AI-related third-party dependencies and service provider concentration: findings from publicly available surveys

The AI surveys carried out by the Bank of England and Financial Conduct Authority in recent years are among the richest sources of publicly available information on AI-related third-party dependencies and service provider concentration.[52] The 2024 survey found that 33% of AI use cases in UK financial services were implemented by third parties, up from 17% in 2022. Additionally, foundation model use cases, which necessarily involve a degree of third-party dependence because the models are pre-trained, account for 17% of AI use cases. The survey also assesses service provider concentration by asking FIs about the top three providers of cloud services, models, and data. Unsurprisingly, the top three cloud service providers account for about three-quarters of cloud usage. Notably, concentration among providers of AI models appears to be growing, as the top three model providers accounted for

[47] DeepSeek (2025), *DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning*, January

[48] As of this writing, 6 of the top 25 LLMs on the LMArena Leaderboard, are published under open-source licenses. These models are developed by DeepSeek, Alibaba, Minimax, and Google. LMArena, Leaderboard, Text, July 1, 2025.

[49] See Gambacorta and Shreeti (2025), *The AI supply chain* BIS Papers, No. 154, March.

[50] See CNBC (2024), Why big tech is turning to nuclear to power its energy-intensive AI ambitions, October

[51] Hart (2025), *Advanced Micro Devices Sets Sights on Nvidia in AI Race*, Wall Street Journal, June; Lin and Huang (2025), *China's Huawei Develops New AI Chip, Seeking to Match Nvidia*, Wall Street Journal, April.

[52] Bank of England and Financial Conduct Authority (2024), November; Bank of England and Financial Conduct Authority (2022), *Machine learning in UK financial services*, October.

44% of named providers in 2024, up from 18% in 2022. Further, the survey asks FIs about the materiality of third-party AI use cases. FIs in the UK rate only about 16% of third-party implementations and 12% of foundation model uses cases as highly material. Finally, FIs ranked critical third-party dependencies as the second most important AI-related system risk, behind cybersecurity.

The Swiss Financial Market Supervisory Authority (FINMA) has also carried out surveys in recent years on AI usage that have included segments on third-party dependencies. In 2022 and 2024, FINMA found that while some firms develop in-house AI applications, most also use external AI service providers, and many smaller institutions rely entirely on service providers for AI applications.[53] The 2024 survey showed that over 90% of respondents that use AI are leveraging generative AI chatbots provided by AI firms.

In 2024, the FSA of Japan conducted a survey of FIs' AI usage patterns, which found that many firms are using vendor-provided AI solutions. Respondents cited several measures to address risk management challenges associated with third-party AI applications, such as leveraging the existing third-party risk management framework, implementing security checks, using open-source options to limit reliance on specific providers, and ensuring proper data security.[54]

Finally, respondents to surveys of capital markets participants carried out by IOSCO and the IMF identified vendor concentration and third-party dependencies as key vulnerabilities associated with AI usage.[55]

## 4.3 Monitoring considerations

The FSB toolkit lays out considerations for identifying systemic third-party dependencies and potential systemic risks relevant for AI adoption by FIs. These include criticality of a service provider and its services to FIs, market concentration in the provision of services, substitutability and the systemic relevance of third-party dependencies. Individually, these considerations do not necessarily pose systemic risks, but their interactions within the context of a service failure could. The considerations most relevant in the context of AI services are laid out below:

- **Critical Service**: An AI service provided to a FI whose failure or disruption could significantly impair a FI's viability, critical operations or its ability to meet key legal and regulatory obligations.[56] Criticality is highly firm specific and may vary over time based on changes in the FI's reliance on that service and changes in its relationship with the service provider. It should be assessed periodically, as it can evolve depending on the FI's business model, service volume and the availability of substitutes.

- **Concentration**: The reliance of FIs, including both large and smaller institutions, on third-party AI services provided by a single or small number of providers is a critical area of focus. Proportionality should be applied, ensuring that oversight and monitoring

[53] FINMA (2025), *FINMA survey: artificial intelligence gaining traction at Swiss financial institutions*, April; FINMA (2023), *Annual Report, 2022*, March.

[54] Financial Services Agency of Japan (2025), *AI Discussion Paper Version 1.0: Preliminary Discussion Points for Promoting the Sound Utilization of AI in the Financial Sector*, March.

[55] See: International Organization of Securities Commissions (2025), ., March, pp. 41-42; International Monetary Fund (IMF) (2024), Advances in artificial intelligence: implications for capital market activities, Chapter 3, October, p. 91.

[56] As defined in FSB (2023), p. 6.

efforts are tailored to the size, complexity and risk posed by the third-party service provider.

- **Substitutability**: AI services that are easily and readily substitutable may be less critical.

- **Systemic relevance of third-party dependencies**: The FSB toolkit emphasises that systemic third-party dependencies arise when the disruption or failure of a service provider's critical services could impact multiple financial institutions or the wider financial system. These dependencies are assessed based on the criticality of the services, the degree of market concentration, and the substitutability of the services provided and the recoverability of the disrupted services.

The FSB toolkit emphasises the importance of a holistic approach to third-party risk management that goes beyond the traditional outsourcing. This approach is particularly relevant to GenAI-related third-party dependencies because of the centrality of open-source software libraries developed by third parties for which FIs have little recourse in the case of material bugs. It is even more critical for monitoring vulnerabilities today given the rising importance of pre-trained models, which often do not involve formal contractual relationships but nevertheless introduce third-party risk.

Assessing concentration-related vulnerabilities in the third-party supply chain is challenging, but the FSB toolkit's provides principles to help identify and mitigate these risks. The toolkit stresses the need to understand the role of key nth-party service providers for critical services. The AI supply chain includes several potentially important nth-party service providers for FIs. For example, while some FIs may rely on hardware purchased directly from chip suppliers, many more have indirect exposure to chip suppliers through their use of cloud services. The complexity of AI supply chains and the limited ability of FIs to monitor AI firms, makes this one of the most difficult areas to assess. The FSB toolkit emphasises the importance of FIs conducting appropriate due diligence, implementing robust monitoring practices, and reassessing third-party relationships to identify and mitigate these risks. Financial authorities can also support these efforts by aggregating data across FIs to better assess concentration risks at a systemic level.

The FSB toolkit highlights the importance of proportionate risk management for both critical and non-critical services to ensure operational resilience across the supply chain. While the toolkit focusses on critical services, it makes clear that risk-based monitoring of non-critical services is important as well. Non-critical services may still pose a range of risks and business impacts if disrupted. Given increasing vertical integration in the AI supply chain (see Box 4), AI service providers may supply a combination of critical and non-critical services.

Surveillance indicators proposed by the FSB toolkit, used by some public authorities, can help authorities monitor AI-related third-party dependencies and service provider concentration. Section 3.2.2 introduced a set of example indicators that authorities can use to assess this vulnerability. Table 3 provides a more in-depth series of indicators and data sources that can help authorities to monitor AI-related third-party dependencies and assess the key criteria for systemic risk outlined in the FSB toolkit. Authorities overseeing the same markets for distinct policy objectives may offer additional valuable insights and data (for example, competition authorities providing input on third-party providers market dynamics) that could meaningfully enrich the monitoring exercise.

**Table 3: Mapping surveillance indicators and data sources to key monitoring areas for AI-related third-party dependencies and service provider concentration**

| Monitoring area | Potential indicators and data sources |
|---|---|
| **Third-party relationships** | • Share of AI applications implemented by third parties<br>• Share of AI applications utilising pre-trained models (e.g. LLMs)<br>• Share of AI applications running off premises<br>• Notifications to authorities by FIs of third-party AI relationships<br>• Review of FIs' registers of third-party AI service providers<br>• Notifications to authorities by FIs of operational incidents affecting third-party AI service providers<br>• Share of overall business applications implemented by third parties that rely on AI (i.e. indirect AI exposure, nth-party risk) |
| **Criticality** | • Registers of critical AI services and service providers based on data and information collected from supervised FIs<br>• Survey questions related to the number of critical third-party AI applications<br>• Critical AI services and service providers listed in FIs' recovery and resolution plans, as available<br>• Where the BCBS Principles for Operational Resilience have been implemented, AI services and service providers listed in banks' maps of "internal and external interconnections and interdependencies" for the delivery of critical operations[57] |
| **Concentration** | • Overall number of AI services supported by a single or closely connected AI service providers<br>• Number of critical AI services supported by a single or closely connected AI service providers<br>• Level of exposure to AI services in specific jurisdictions or regions<br>• Market share of AI service (model, hardware, infrastructure, data) providers in the financial sector<br>• Key AI supply chain dependencies obtained by FIs from their service providers through due diligence and ongoing monitoring |
| **Substitutability** | • Relative cost and performance of widely used AI services<br>• Estimates of switching costs and time to switch between AI services<br>• Number of competitive service providers in relevant markets (model, hardware, infrastructure, data)<br>• Number of firms using vertically integrated AI systems |
| **Systemic importance of firms** | • Number of global or domestic systemically important FIs for which third-party AI services support critical operations |

[57] BCBS (2021), *Principles for Operational Resilience*, March, p. 6.

| Monitoring area | Potential indicators and data sources |
|---|---|
| | • Share of financial sector assets owned by FIs for which third-party AI services support critical operations |

## 5 Conclusion

This report examines the monitoring of AI adoption and associated vulnerabilities, recognising its critical role in enabling authorities to address vulnerabilities such as third-party dependencies, while fostering safe and sound innovation. Such efforts are essential to fully harness the potential benefits of AI, including enhanced efficiency, improved regulatory compliance, advanced data analytics, and the creation of more personalised financial products.

The results from the member survey reveal that most financial authorities are collecting data on AI adoption, but many are still in an early stage of monitoring AI-related financial sector vulnerabilities. Current efforts largely rely on industry surveys, outreach, and publicly available data. Several data collection challenges remain, including fragmented indicator sources, inconsistent definitions, high costs, resource and skills constraints, and difficulties in assessing the criticality of AI services. In addition, AI adoption in the financial sector is still evolving, consistent with the broader evolution around deployment of AI throughout the global economy. Mapping indicators to specific vulnerabilities, ensuring regular data collection, and addressing gaps in monitoring critical areas such as third-party dependencies, market correlations, and cyber risks will help to enhance monitoring initiatives. Most authorities have plans to enhance their AI-related data collection initiatives.

To assist member authorities' efforts in addressing the above challenges, the report identifies key considerations for improving monitoring approaches, including mapping indicators to vulnerabilities, minimising collection burdens, improving representativeness and timeliness, and aligning with relevant standards. The report also underscores the importance of leveraging both direct and proxy indicators, combining quantitative and qualitative data sources, flexibly utilising existing frameworks and tools, exploring in-depth supervisory engagements, and fostering collaboration across functional authorities and across borders.

The case study on third-party dependencies and service provider concentration shows that while some authorities monitor GenAI-related third-party relationships through surveys, less progress has been made in assessing criticality and concentration risks. Authorities could leverage the FSB's third-party risk management toolkit to develop indicators and frameworks for monitoring these vulnerabilities. The toolkit provides practical strategies for assessing criticality and identifying systemic third-party dependencies, as well as tools for monitoring and managing risks associated with these dependencies.

Looking ahead, authorities may consider several ways to address data gaps and develop more robust monitoring approaches to assess relevant vulnerabilities. To this end:

- National authorities should consider ways to enhance monitoring approaches as they see appropriate, in line with the considerations presented in this report, including:
  - Collaborating with domestic stakeholders to formalise metrics aimed at monitoring and assessing vulnerabilities, building on the indicators presented in this report;

  - Enhancing supervisory engagements with FIs to gain more in-depth insights into AI related vulnerabilities, particularly those vulnerabilities where it is more challenging to identify quantitative indicators;
  - Exploring the use of AI tools to enhance monitoring capabilities; and
  - Engaging with AI firms and other relevant entities where appropriate to enhance understanding on AI adoption and associated vulnerabilities.

- National authorities could seek a more comprehensive understanding of AI usage in the financial sector by fostering greater data sharing across domestic sectoral financial regulators. Further sharing of information and experiences with non-financial authorities domestically could also help enhance monitoring efforts.

- The FSB and relevant SSBs can support domestic efforts by fostering cross-border cooperation to facilitate sharing of information, experiences, and good practices including in supervisory engagements with FIs. They could also work towards greater alignment in taxonomies and indicators where relevant and feasible. Such efforts would promote a more consistent and comprehensive understanding of AI adoption and related vulnerabilities across the global financial system, while also leveraging the SSBs capacity building initiatives.

- The FSB and relevant SSBs are encouraged to continue monitoring AI developments and addressing remaining data gaps. This includes exploring ways to assess vulnerabilities that are particularly challenging to monitor such as market correlations, model risks, data quality and governance, and misaligned AI systems.

The findings of this report highlight the importance of monitoring vulnerabilities associated with AI adoption. These findings will help inform future FSB work on AI.

# Glossary

This glossary provides a (non-exhaustive) list of terms used in the report. Many of these terms are commonly used in the field of AI and 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 in other contexts. Where applicable, some terms align with the definitions set out in the FSB Toolkit to ensure consistency with established frameworks and practices.

**Agentic AI:** Systems designed to autonomously perform complex and extended tasks, often making decisions and taking actions with limited human oversight. These systems are distinct from generative AI but may incorporate generative capabilities to enhance content generation and decision making.

**Algorithm:** 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.

**Critical Service**: An AI service provided by a third-party service provider to a FI whose failure or disruption could significantly impair a FI’s viability, critical operations or its ability to meet key legal and regulatory obligations. Criticality is firm specific and may vary over time based on changes in the FI's reliance on that service and changes in its relationship with the service provider.

**Criticality:** The importance of a service, system, or provider to the operations of a financial institution.

**Data and model poisoning:** An attack where malicious actors manipulate training data or model parameters to introduce errors or biases into an AI model's outputs. This can compromise the integrity, reliability, and security of AI systems.

**Data-network-activities (DNA) loop:** A feedback mechanism where entities with extensive data pipelines continuously improve services, attract users, and generate more data. This reinforces economies of scale and strengthens control over high-quality data.

**Deep learning:** A form of machine learning that uses algorithms that work in ‘layers’, inspired by the structure and function of the brain. Deep learning algorithms can be used for supervised, unsupervised, or reinforcement learning.

**Direct Indicators:** Specific and measurable data points that provide clear, granular insights into a phenomenon

**Disinformation:** The deliberate creation and dissemination of false or misleading information, with the intent to deceive or manipulate public opinion, market behaviour, or decision-making.

**Explainability:** The ability of an AI model to provide clear and interpretable outputs or decisions.

**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 usually 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. Key tasks LLMs perform include text generation, document classification, summarisation, question-and-answer, and sentiment analysis, among other tasks.

**Learning:** The process by which a machine learning model or agent improves its performance on a task over time by identifying patterns, relationships, or strategies within data or from interactions. This involves adjusting its internal parameters (e.g., weights in neural networks) to optimise outcomes, such as making accurate predictions, taking effective actions, or achieving specific goals

**LLM hallucinations:** Occur when a large language model (LLM) generates seemingly confident but inaccurate outputs, or fabricates nonsensical outputs in response to user inputs.

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

**Misinformation:** The unintentional sharing of false or inaccurate information, often due to lack of verification or understanding.

**Misaligned AI systems:** AI systems whose objectives, outputs, or decision-making processes deviate from intended standards, principles, or regulations set by its developers or users.

**Model Risk:** The potential for adverse consequences arising from decisions based on incorrect or misused models.

**Nth Party:** An entity within the supply chain of a third-party service provider that indirectly supports the delivery of services to the FI.

**Open-source models:** AI models where the full training code, and in some cases the training data or its composition, is made publicly available for use and modification. These models offer customisability and reduce vendor lock-in but may introduce additional risks, such as security vulnerabilities or data quality concerns.

**Open-weight models:** AI models that disclose their learned parameters (weights and biases), enabling developers to fine-tune them for specific applications. These models enhance flexibility and reduce dependence on proprietary solutions, offering deployment options that mitigate concentration risks in the AI ecosystem.

**Operational resilience:** The ability of a financial institution to deliver its critical operations through disruptions. This includes the capacity to prepare for, withstand, respond to, recover from, and adapt to adverse events, ensuring the continuity of critical services.

**Proxy Indicators:** Indirect measures used to infer information about a phenomenon when direct data is unavailable or difficult to obtain.

**Reasoning models:** AI systems designed to perform multi-step reasoning tasks by breaking problems into sub-parts and solving them in a structured manner. These models are emerging as a key innovation in AI development, enabling the execution of complex tasks with improved inference capabilities.

**Reinforcement learning:** A subset of machine learning which falls in between supervised and unsupervised learning. 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:** The algorithm is fed a set of 'training' data that contains labels on all of the observations. For instance, a data set of transactions may contain labels on 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 observations when deployed on a data set.

**Switching Costs:** The financial, operational, or strategic barriers that organisations face when transitioning from one service provider or solution to another.

**Systemic Relevance:** The potential impact that the failure or disruption of a service, provider, or dependency could have on the broader financial system.

**Systemic third-party dependencies:** Dependencies on one or more external service providers whose failure or disruption could significantly impair the ability of multiple financial institutions to deliver critical services, potentially leading to risks for financial stability. These dependencies arise when critical services provided by a single or limited number of service providers are highly concentrated, lack substitutability, or have interdependencies within their supply chains.

**Traditional AI:** A suite of computational techniques that pre-date recent advances, such as GenAI.

**Unsupervised learning:** 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.

**Vertical integration:** The consolidation of multiple stages of a supply chain or production process within a single organisation. In the context of AI, vertical integration occurs when one company controls various layers of the AI supply chain, such as hardware, cloud infrastructure, and AI models, offering end-to-end services.

# Abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| AIPPF | Artificial Intelligence Public Private Forum |
| AMD | Advanced Micro Devices |
| AWS | Amazon Web Services |
| BCBS | Basel Committee on Banking Supervision |
| BIS | Bank for International Settlements |
| BOE | Bank of England |
| BTOS | Business Trends and Outlook Survey |
| CONSOB | Commissione Nazionale per le Società e la Borsa |
| COVIP | Commissione di Vigilanza sui Fondi Pensione |
| CPMI | Committee on Payments and Market Infrastructures |
| DNA | Data Network Activities |
| ESMA | European Securities and Markets Authority |
| EU | European Union |
| FCA | Financial Conduct Authority |
| FI | Financial Institution |
| FIRE | Format for Incident Reporting Exchange |
| FPC | Financial Policy Committee |
| FSB | Financial Stability Board |
| FSI | Financial Stability Institute |
| GenAI | Generative Artificial Intelligence |
| GFSR | Global Financial Stability Report |
| GPU | Graphics Processing Unit |
| G-SIB | Global Systemically Important Banks |
| IAIS | International Association of Insurance Supervisors |
| IMF | International Monetary Fund |
| IOSCO | International Organisation of Securities Commissions |
| IVASS | Istituto per la Vigilanza sulle Assicurazioni |
| JFSA | Financial Services Agency of Japan |
| LLM | Large Language Model |
| OECD | Organisation for Economic Cooperation and Development |
| R&D | Research and Development |

| | |
|---|---|
| RFI | Request for Information |
| SSB | Standard Setting Body |
| TSMC | Taiwan Semiconductor Manufacturing Company |
| WIPO | World Intellectual Property Organisation |