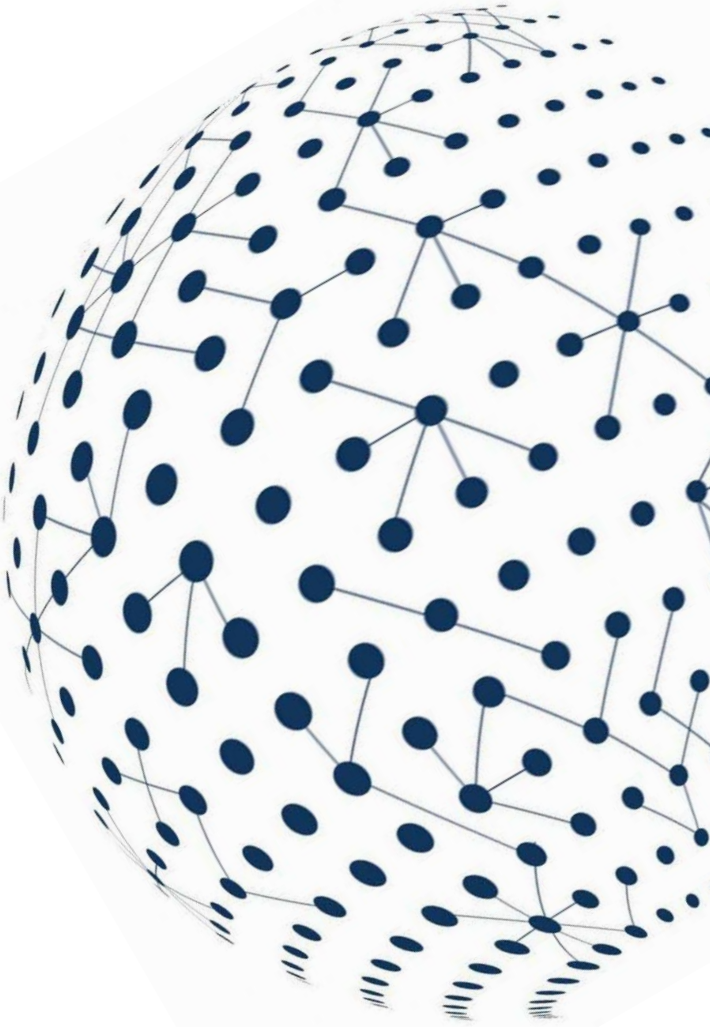
FSB FINANCIAL STABILITY BOARD

Sound Practices for Responsible Adoption of Artificial Intelligence (AI)

Final report



15 October 2026

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

Contact the Financial Stability Board

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

Copyright © 2026 Financial Stability Board. Please refer to the terms and conditions

Table of Contents

Executive summary 1

Introduction 3

1. An overview of the use of AI in the financial system 5

    1.1. AI adoption in the financial sector 5

    1.2. Use cases and benefits of AI in the financial system 6

    1.3. Risks and implementation challenges of AI adoption for financial institutions 13

2. Organisation-wide AI governance 20

    2.1. Strategic direction and oversight 20

    2.2. Governance and accountability 22

    2.3. AI risk management framework and effective documentation 24

    2.4. Organisational adaptability 27

3. AI lifecycle management 30

    3.1. Stages of AI development and deployment 30

    3.2. Materiality and risk assessment 31

    3.3. Selection process 33

    3.4. Data governance 35

    3.5. Explainability and transparency 38

    3.6. Performance management 43

    3.7. Human oversight 49

    3.8. Cyber and ICT risk management 55

    3.9. Third-party AI risk management 60

Annex: List of Sound Practices for financial institutions' responsible AI adoption 65

Glossary 66

References 68

Executive summary

Financial institutions are rapidly adopting and innovating with Artificial Intelligence (AI) to improve efficiency, transform their business models, enhance customer services and strengthen risk management. As adoption expands in scale and sophistication, AI may also amplify existing risks and introduce new ones, with implications for financial stability. For example, less explainable models can undermine transparency, while highly autonomous agentic AI systems may act unpredictably or outside intended boundaries, potentially resulting in unauthorised or erroneous actions, data security incidents and disruption to connected systems. Some advanced models may also materially increase the speed and scale of cyber attacks.

Responsible AI adoption enables financial institutions to harness opportunities and benefits while minimising associated risks. This means that financial institutions need to understand the opportunities and risks of AI as well as respond with the appropriate strategy and guardrails. Responsible AI adoption can also reduce risks to financial stability. Financial institutions should also be cognisant of the risks of not adopting AI such as reduced competitiveness and diminished capacity to detect and manage cyber threats.

The Financial Stability Board (FSB) has identified 12 sound practices to help all financial institutions realise the benefits of AI while managing its risks responsibly. The report includes case studies illustrating the benefits that financial institutions have reported and how some sound practices have been applied proportionately. These case studies are illustrative in nature and are not intended to prescribe a specific approach to AI adoption nor do they represent expected outcomes or benchmarks for any financial institution.

Financial institutions should consider proportionality when applying the sound practices. More robust practices may be appropriate for financial institutions that are large, complex or highly connected within their ecosystem and where AI is used or deployed in the financial institutions' critical functions. Smaller, less complex, or less interconnected financial institutions and less material or lower risk use cases within financial institutions may warrant application of only relevant sound practices or appropriate modification of the relevant sound practices.

The 12 sound practices are organised into two groups. The first four sound practices emphasise the importance of organisation-wide AI governance as financial institutions adopt AI. These four sound practices highlight: (i) the pivotal role the board and senior management play in setting the overall approach and providing oversight so that AI adoption is aligned with the financial institution's business model, risk appetite and strategy; (ii) maintenance of an appropriate governance framework with well-defined roles and responsibilities; (iii) incorporation of AI risks into the risk management framework and effective documentation of AI use; and (iv) undertaking continuous learning and adaptation.

The subsequent eight sound practices set out a comprehensive framework for managing risks throughout the AI lifecycle, from inception to retirement. These sound practices focus on: (v) effective and systematic assessment of the materiality and risks associated with AI use cases at inception and thereafter; (vi) selection of appropriate AI technologies; (vii) appropriate data governance; (viii) the explainability of various types of AI and consideration of compensating controls; (ix) evaluation of the performance of AI use cases; (x) appropriate and effective human

oversight; (xi) management of AI-related cyber and information and communication technology (ICT) risks; and (xii) management of risks from third-party AI dependencies.

The board and senior management of financial institutions are strongly encouraged to reference these sound practices when developing and refining their institution's AI governance, risk management and control frameworks, including as AI adoption expands over time. The sound practices are non-prescriptive and do not constitute a binding international standard. Rather, they serve as a practical toolkit that financial institutions can tailor to their specific context and risk profile, and integrate into existing frameworks where appropriate, including those for cyber and third-party risk.

The sound practices also aim to promote coordination, cooperation and information-sharing among financial institutions, supervisors and other stakeholders, within and across jurisdictions. They build on, and are broadly compatible with, existing and ongoing work by the FSB and other standard-setting bodies (SSBs). As AI technologies and applications evolve, the FSB will monitor developments and update the sound practices as necessary to support safe and responsible AI adoption by financial institutions.

Introduction

Financial institutions have long used artificial intelligence (AI)[1] tools, but rapid advances - particularly in generative AI (GenAI) and agentic AI - have generated significant interest.[2] Financial institutions are increasingly adopting, using and innovating with AI ('AI adoption') across a wide range of activities, including credit risk assessment, trading, portfolio services and investment operations, fraud prevention, transaction monitoring, market surveillance, customer service, coding assistance and document review and summarisation.

AI is transforming financial services and business models. Its applications range from automating repetitive tasks to supporting complex decision making and execution. More recently, financial institutions have shown increasing interest in the use of AI agents that can operate autonomously across end-to-end-processes. These developments are reshaping how financial institutions operate, innovate, and serve customers by improving efficiency, reducing costs and widening access to financial products and services.[3]

At the same time, AI may also amplify existing risks or introduce new ones that need to be identified and managed appropriately.[4] For example, complex and less explainable types of AI could increase model risks for financial institutions, while autonomous AI systems may take unauthorised or erroneous actions. Financial institutions may also need to consider the implications of not adopting AI, including reduced competitiveness and a diminished ability to detect and manage threats such as financial fraud. In some areas, AI presents both opportunities and risks. It can increase the ease, speed, frequency and impact of cyber attacks,[5] while also strengthening financial institutions' cyber defence capabilities.

Responsible AI adoption enables financial institutions to harness opportunities and benefits while minimising associated risks. This means that financial institutions need to understand and remain updated on the opportunities and risks of AI and respond with the appropriate adoption strategy and guardrails to manage evolving associated risks. At the financial system level, responsible AI adoption reduces the risks to financial stability.

To facilitate responsible AI adoption by financial institutions, the Financial Stability Board (FSB) has developed this report which sets out 12 sound practices financial institutions are encouraged to consider.

The structure of the report is as follows:

- Section 1 highlights the benefits and risks associated with AI use in the financial system;
- Section 2 presents sound practices for organisation-wide AI governance;

---

1 For detailed AI-related terms and their definitions, please refer to the Glossary section.

2 For example, see Breeden (2026).

3 See Bowman (2026).

4 See, for example, FSB (2024b).

5 This includes risks from the misuse of AI models with the autonomous capabilities to discover and generate working exploits for security vulnerabilities.

- Section 3 presents sound practices for managing AI throughout its development and deployment (AI lifecycle[6]);
- Annex lists the 12 sound practices for easy reference; and
- the report concludes with a glossary of key terms and a list of references.

The board and senior management of financial institutions are strongly encouraged to reference the sound practices as they consider business strategy, technology adoption and risk management in an increasingly AI-enabled environment. In doing so, they should note the following:

- While all sound practices in this report are generally applicable to all types of AI, certain practices can be more relevant for specific AI technologies – for example, practices addressing risks arising from the autonomy of AI agents.
- The sound practices are not exhaustive and will evolve as AI technologies and understanding of their associated risks develop. In particular, sound practices specific to agentic AI and multi-agent systems remain nascent and may warrant more comprehensive treatment in the future.
- The sound practices should be applied proportionately. Each financial institution should consider the relevance and applicability of these sound practices based on its business model, complexity, role in the financial system, structure, size and the extent to which AI is used or deployed in their critical (or material) functions. Financial institutions may also adapt certain sound practices, depending on the materiality and risk of a specific AI use case, impact and outcomes of the use case and the type of AI being adopted.
- The report includes case studies illustrating reported benefits of AI adoption and how financial institutions have applied some of the sound practices proportionately. These case studies are illustrative only and do not prescribe a specific approach to AI adoption nor do they represent expected outcomes or benchmarks for any financial institution.

This report builds on, and is broadly compatible with, existing and ongoing work by the FSB[7] and other SSBs, as well as by national/regional financial authorities ('authorities'). It also draws on inputs from a range of stakeholders across the financial system, including financial institutions and technology vendors, as well as feedback received through the public consultation on the earlier version of this report published in June 2026.[8]

In response to the consultation feedback, the report expands its description of benefits and risks. It recognises the role of AI as an augmentative technology and workforce multiplier, while highlighting the risk of workforce deskilling. It also addresses documentation needed to support auditability, traceability, sound governance and effective oversight. Several sound practices have also been enhanced. Key updates include: clearer descriptions of the roles of boards and

---

6 There is no standard, one-size-fits-all stages of AI lifecycle as different AI use cases may involve different stages of varying length. For details, see Section 3.1.

7 See FSB (2024b) and FSB (2025b).

8 All public consultation responses are available on the FSB website. See FSB (2026).

senior management, including considerations for smaller financial institutions; additional guidance on effective documentation; greater emphasis on transparency for higher-risk and higher-material use cases; and broader coverage of third-party AI risk management. The report also now includes additional considerations for managing advanced risks associated with agentic AI and multi-agent systems. These considerations may evolve as understanding of these technologies develops and may warrant more comprehensive treatment in the future.

The sound practices do not establish an international standard, prescribe how financial institutions should adopt AI, nor are they intended to influence business decisions to adopt a particular AI technology. Applying the sound practices in this report also does not absolve a financial institution from its obligations to meet local legal and regulatory requirements related to AI adoption.

1. An overview of the use of AI in the financial system[9]

1.1. AI adoption in the financial sector

AI is increasingly transforming financial services through a wide range of use cases. Financial institutions are leveraging AI in areas such as anti-money-laundering (AML) and know-your-customer (KYC), credit risk, cyber security, customer engagement, fraud detection, optimising internal processes, collateral and portfolio management and regulatory compliance. These applications have the potential to deliver value by enhancing the analysis of data and information, improving risk monitoring and management and supporting faster and more accurate decision-making across front and back-office functions, whilst reducing operational costs.[10]

This transformation is driven by both supply and demand-side factors. On the supply side, advances in computing capabilities and power (including through cloud infrastructure), the growth of available data and greater availability of foundation models have lowered barriers to adoption. On the demand side, financial institutions seek to boost their competitive position in increasingly digital markets, improve operational efficiency and strengthen risk management.

AI has shown significant advancements in the last decade. Beyond traditional AI and machine learning (ML), which learns from data to make predictions, recommendations, or decisions, recent years have seen the emergence of large language models (LLMs), which can analyse and generate human language by processing vast amounts of text data and GenAI, which can create new, often multimodal content (audio, images, text, video). More recently, agentic AI has emerged whereby autonomous systems (‘agents’) are capable of planning, reasoning and executing complex high-level goals (comprising multiple tasks) independently. These forms of AI are not exhaustive list, and other forms may exist or emerge.

While risks posed by AI adoption are not all new, some risks could be accentuated and there are some newer risks specific to certain forms of AI technologies, such as highly autonomous agentic AI. The FSB and relevant SSBs emphasise proportionate, risk-based and technology-neutral approaches to monitoring and addressing risks, and some SSBs have issued

---

9 This Section draws on existing publications by the FSB, SSBs, and other authorities as well as market participants, researchers, and media. It also drew on inputs from engagements with external stakeholders.

10 See, for example, BCBS (2024), BIS-FSI (2025a), Bowman (2024), Breeden (2024) and Machado (2026).

guidance specific to AI.[11] As such, authorities, whilst supporting AI adoption, stress the importance of responsible AI adoption via strong governance, clear accountability and sound risk management practices especially in high-materiality and high-risk use cases.[12]

The FSB assessed the financial stability implications of AI in the financial system in 2017, followed by an update in 2024.[13] However, given the rapidly evolving nature of the technology, the benefits and challenges set out in this section remain subject to future reassessment by the FSB.

1.2. Use cases and benefits of AI in the financial system

AI adoption has accelerated since the 2024 FSB report on the financial stability implications of AI,[14] though this acceleration varies across entities, sectors and jurisdictions. Evidence from surveys and industry engagement by authorities[15] suggests that internationally active banks, large or sophisticated trading firms and asset managers and payment providers show relatively advanced use. In addition, several AI use cases cut across financial activities, such as general AI productivity tools and the use of AI to boost the efficiency of back and middle-office functions and risk management.[16]

- **Banking.** Banks are generally progressing rapidly in embedding AI in operational and risk management functions. This includes the use of traditional AI in credit risk management, document automation, fraud detection and internal controls. Adoption in front office functions for core financial decisions remains more cautious, reflecting concerns around explainability and heightened risk considerations.

- **Insurance**. Insurers have historically relied on rule-based systems, which are gradually being replaced or complemented by more sophisticated AI-driven approaches. There is evidence of growing use of AI in claims-handling, customer segmentation, fraud identification and underwriting, though adoption varies by jurisdiction and is often shaped by risk considerations.

- **Capital markets and asset management**. Quantitative trading firms and large asset managers are early adopters of traditional ML in areas such as portfolio optimisation and analysis of alternative data. Adoption across the industry varies and some industry participants plan to increase AI adoption over time. Current use cases include: algorithmic and high frequency trading; customer service and research; market-surveillance; trade monitoring; portfolio services and investment operations; pattern recognition; sentiment analysis; and volatility forecasting.

---

11 See FSB (2025b), IOSCO (2025) and IOSCO (2026).

12 For example, see MAS (2024), HKMA (2024), HKMA (2025), JFSA (2021), FINMA (2024), and OSFI (2023).

13 See FSB (2017) and FSB (2024b).

14 FSB (2024b).

15 See BOE website.

16 For example, see IMF (2024), and Hlophe and Mabetha (2025).

- **Payments**. AI integration is especially strong in customer facing use cases such as behavioural risk analytics, onboarding and KYC. Regarding KYC, financial institutions have reported improvement in both the accuracy and processing speed of KYC checks.

- **Financial market infrastructures (FMIs)**. FMIs are exploring a range of use cases, including the detection of anomalous transactions and data inconsistencies and AI-driven market surveillance, settlement, reconciliation and compliance systems. Some FMIs are also exploring or implementing use cases involving predictive analytics for enhanced stress testing and development of credit default early-warning indicators to enable early detection of vulnerabilities.

Credit scoring

In credit scoring, AI is being adopted to improve accuracy through advanced analytics applied to large volumes of financial and behavioural data. Banks are using different types of AI models, such as decision-trees and neural networks, which may be developed in-house or provided by a third-party. These models may be hosted on premise or on an external cloud infrastructure. In some jurisdictions, smaller financial institutions are partnering with AI providers to develop AI credit scoring tools.

AI-based credit scoring can allow lenders to better assess credit risk where traditional methods are less effective and when paired with alternative data, broaden consumer access to financial services or products.[17]

Some banks are also using AI to enhance credit underwriting, particularly for small and medium-sized enterprises (SMEs). In several jurisdictions, GenAI-enabled tools have been deployed to automate data extraction from financial documents and generate structured narratives supporting credit decisions, contributing to reduced processing times, improved consistency in credit assessments and enhanced overall operational efficiency in credit risk management functions. Several banks have developed traditional AI credit decision models, particularly in their credit card and auto loan portfolios. These applications often combine AI methodologies, such as gradient boosting machines or neural networks, with alternative data to support decisions to approve or decline new credit requests (or requests for credit line increases). This has enabled banks to improve risk profiling, which may contribute to lower default rates and expanded credit access, particularly for borrowers who may not qualify under traditional credit assessment methods.

Case study: AI for credit risk management

A large regional bank has systematically embedded ML into its credit risk operations, especially in SME lending, where the bank's ML models proactively generate alerts for borrowers showing early signs of cashflow deterioration. In 2022, the bank successfully identified over 95% of non-performing SME loans at least three months before the businesses experienced issues meeting their debt repayments. This allowed the bank to engage with at-risk SMEs early to understand their situation and partner with them to explore possible pre-emptive solutions - such as restructuring repayment

[17] Alternative data generally refers to information that is not typically found in the consumer's credit file of the nationwide consumer reporting agencies or information not customarily provided by consumers as part of the applications for credit. Such alternative data can include payment behaviour, cash flow data, or non-traditional financial information. See FRB et al (2019).

schedules or adjusting credit facilities - before credit issues worsened. As a result, over 80% of identified at-risk borrowers were averted from default altogether. These outcomes allowed more accurate and timely assessment of credit risk across a large and diverse borrower bases and allowed the bank to provide early support to customers while improving the overall quality of its loan portfolio.

Beyond assessment of credit risk, GenAI is also being applied to streamline credit underwriting processes. Another medium-sized regional commercial bank developed an 'AI Approver Assistant' by integrating GenAI into SME credit underwriting. The solution uses GenAI to automate data extraction, generate credit narratives and support risk detection, aiming to streamline approval processes, enhance decision-making consistency and establish a scalable governance and operating model. It achieved over 80% accuracy in financial data extraction, with credit approvers rating more than 70% of GenAI-generated content as valuable reference material. Processing time for preliminary credit proposal generation was reduced from more than a day to 15 minutes and the system matched manual review performance in identifying data inconsistencies and potential fraud signals across all test cases.

Trading, asset management and portfolio optimisation

The adoption of AI by financial institutions is supporting a range of investment and trading activities including: automated portfolio reporting; sentiment analysis (e.g. for parsing earnings calls); liquidity forecasting and volatility modelling; credit risk analysis; pattern detection; and signal extraction from alternative data. Recent research indicates that AI adoption is yielding productivity improvements and cost savings in trading algorithm design, better data processing and, in some cases, discovery of new investment opportunities.[18] While there is little evidence at present of GenAI being used for fully autonomous trading,[19] financial institutions are exploring the use of agentic AI, which can autonomously sequence trading-related tasks (e.g. scanning news, generating signals and preparing execution instructions), potentially enabling more streamlined workflows and reduced manual intervention.

Building on these developments, evidence from industry practices illustrates how financial institutions are applying AI in specific investment and trading contexts. For example, some asset management companies, notably those active in the private equity sector, make use of AI-supported investment opportunity identification tools to broaden the set of opportunities available to investment teams engaged in research and portfolio construction. Some large internationally active banks and institutional broker-dealers have recently adopted research and analytics assistants to enhance trader workflows. These solutions often customise AI assistant applications and leverage AI-powered agents to support traders in their market analyses. For example, a research agent can compare different hedging strategies by analysing several market data sources in real time, while AI-powered assistants may also have access to a variety of system tools that enable them to visualise outcomes and conduct statistical analysis. Initial results suggest that accelerated analysis can lead to significant time savings, supporting more efficient decision-making processes and streamlined trading workflows.

---

18 See Lim et al (2025).

19 See FMSB (2026).

Case study: Investment risk assessment with AI

A global asset manager developed an AI application in response to the growing complexity of investment proposals, particularly in private markets, and increasing pressure on risk teams to deliver faster, more consistent and well-documented assessments. The application was designed to accelerate the largely manual process of translating an investment memorandum into an initial risk assessment.

Acting as an intelligent assistant, the application reviews investment documentation, identifies relevant information and assesses proposals against approved mandate rules. It produces a structured initial risk assessment that highlights potential concerns and provides supporting evidence for the risk manager's consideration. Its outputs are linked to the applicable rules and source documents, supporting transparency and effective oversight. The application does not approve or reject investments and final accountability remains with the risk manager.

The application enables risk teams to produce an initial risk assessment within hours and apply a more consistent approach across proposals. This allows risk managers to focus on more judgement-intensive analysis and challenge, rather than repetitive document review. The asset manager is exploring how the application could be extended across the investment lifecycle, including early risk screening, due diligence, investment committee reporting, post-investment monitoring and benchmarking against past transactions.

Regulatory compliance, AML/CFT and fraud detection

Several financial institutions are using AI to improve fraud detection and financial crime monitoring by analysing large volumes of transactions and unstructured data. Some forms of traditional AI (e.g. neural networks and random forest algorithms) can enhance anomaly detection and help uncover hidden relationships between transactions, strengthening monitoring capabilities. AI can enhance AML/KYC checks by automating document verification, identity checks and fraud detection. Techniques such as biometric verification and contextual analysis can strengthen security, reduce manual work and enhance the overall customer experience. AI is also increasingly used to detect identity fraud, synthetic identities and deepfake-based cyber attacks often in real-time. Authorities have noted reductions in false positives and negatives and better identification of complex criminal patterns.[20]

Some large asset management companies, for example, deploy their AI tools to support compliance reviews of marketing materials. These applications enhance the speed, consistency and quality of compliance checks across marketing and disclosure documentation. Some large FMIs, notably exchanges, also apply AI for market surveillance and abuse detection, analysing internal and external data sources to strengthen detection capabilities and improve the efficiency of monitoring and compliance activities. Various types and sizes of financial institutions (e.g. banks, payment service providers) widely use ML models for fraud prevention in payment transactions. These tools enable real-time analysis of large transaction volumes, supporting faster detection of suspicious activity and improving the overall security and efficiency of payment services. Some medium to large financial institutions report the use of GenAI tools in financial crime and AML investigations. By correlating information from multiple sources and generating investigative narratives, these applications deliver significant time savings and improve consistency and quality in investigative reporting.

[20] See BCBS (2024) and BIS (2025).

Case study: Fraud detection with agentic AI

A large internationally active bank has deployed an agentic AI system to detect emerging fraud and scam patterns in real time, demonstrating measurable improvements in financial crime prevention at scale. Building on its existing AI capabilities (that monitored more than 80 million signals each day, spanning transactions, card and online payments, as well as interactions across digital banking channels), the bank developed an agentic AI system specifically designed to identify emerging threats and autonomously propose the detection rules needed to intercept them. The system was built in-house by the bank's data science and engineering teams in three months, running on a cloud-based data platform and core banking infrastructure to enable real-time data access at scale.

The agent operates continuously, assessing the severity of suspicious patterns, analysing context and generating proposed detection rules for review. The process embeds human oversight to review and approve all new rules by the bank's fraud analytics team before implementation.

The agent has contributed to developing or updating three quarters of the bank's card fraud rules and helped reduce fraud losses by over 20% in the first half of the 2026 financial year compared to the same period in 2025. Daily, the bank processes millions of payments and sends thousands of proactive fraud warning alerts to customers through its mobile banking application.

Separately, a digital bank enhanced its existing facial recognition solution, originally designed to compare facial images against a customer database for digital fraud detection. The solution adds the ability for the bank to detect suspicious image backgrounds in facial recognition images, such as those associated with mule accounts[21] or fraudulent identity attempts. The system extracts facial feature vectors for rapid one-to-many comparison while simultaneously applying object detection and background similarity analysis to flag potential risk indicators. This represents a notable instance of using AI in defence, where the bank leverages advanced technology to counter AI-generated content and evolving fraud vectors.

The enhancement establishes a risk alert mechanism that enhances detection of digital fraud activities including account takeover, deepfake or injection attacks and loan applications involving fake identities. The combined approach, leveraging both facial comparison and image background analysis, supports network analysis of fraudulent activities and strengthens the bank's overall AML and fraud investigation framework, with comparison processes completed in seconds.

Customer-focused applications

AI is increasingly used across some financial institutions to enhance customer engagement in the areas of portfolio management, marketing and customer service. By analysing high-dimensional datasets and automating routine decision-supporting tasks, AI can enhance existing processes and improve customer engagement through tailored financial advice. Some financial institutions are also experimenting with LLM-enabled tools for internal knowledge retrieval, automating customer complaint triage and document classification, which can significantly enhance operational efficiency.[22]

Several financial institutions are increasingly using AI to support robo-advisory services, including for customer profiling, investment planning, portfolio management and rebalancing. Some asset managers are also leveraging AI to enhance their customer advisory services by

[21] Accounts used to facilitate the movement of illicit funds, often in connection with fraud or money laundering.

[22] See, for example, ECB (2024), OSFI (2023), OSFI (2025a), OECD (2024) and OECD (2026).

automating data collection, market analysis and monitoring, reducing costs and expanding services such as real-time insights.

In customer service, AI-driven chatbots and virtual assistants can handle routine queries, payments and loan requests, improving response times, service availability and customer satisfaction, while reducing reliance on call centres. AI is also widely used in marketing activities, to optimise new product campaigns, generate customer leads and create marketing content.

Case study: Customer service with AI

A global systemically important bank (G-SIB), active in both retail and wholesale banking, has piloted an integrated AI application to transform how its corporate relationship managers serve clients.

To address significant time pressures faced by relationship managers in preparing for client engagements, the bank built an AI platform that integrates a wide range of external data sources, including news feeds and research reports, alongside internal knowledge bases. The output from the platform supports corporate relationship managers in developing a better understanding, designing solutions and producing proposals for their clients.

AI-assisted insight generation and proposal creation have reduced preparation time by approximately 50%, while enabling around three times more client dialogue. Critically, the platform has enabled the corporate relationship managers to serve every client, including those who were previously underserved, with updated, tailored insights and proposals.

One large internationally active insurer has used AI to enhance customer service by streamlining and automating the processing of simple insurance claims. The insurer uses optical character recognition to extract relevant information from supporting documents submitted by customers, such as invoices. AI models then validate key fields, such as invoice dates and policy numbers, against policy data. Where the system has insufficient confidence, the claim is referred to a human expert for review.

This has enabled simple, routine claims to be processed and paid within a few hours of filing, with approximately half of claims in one of the insurer's business lines processed fully automatically. To facilitate transparency, the insurer also updated its privacy notices to explain when claims processing may be fully automated and to provide customers with access to human support where needed.

Productivity enhancing applications

Several financial institutions are finding efficiency and productivity gains from AI as it enables the automation of labour-intensive activities, supporting faster execution, more consistent processes, lower operational costs and allowing staff to focus on higher-value tasks. These applications position AI as an augmentative technology and workforce multiplier, supporting staff in performing tasks more efficiently while retaining human judgement, expertise and oversight, particularly for more complex cases. Evidence points to significant productivity gains, particularly from GenAI applications that synthesise and transform unstructured content.[23] Some financial institutions are increasingly using AI to modernise internal operations, including back-office automation, risk analytics, content and code generation and risk management. Foundation models also support large-scale analysis of unstructured data and are being used to strengthen internal controls through automated documentation, monitoring and anomaly detection.[24]

---

[23] See ECB (2024).

[24] See MAS (2025b), HKMA (2024), HKMA (2025), and OSFI (2025b).

Some financial institutions are increasingly adopting AI to support the scaling of operations in environments characterised by growing data volumes and transaction complexity. By enabling the automation and processing of large datasets, AI supports financial institutions in expanding their operational capacity while maintaining service quality.

Several financial institutions globally have reported usage of GenAI tools to boost internal productivity, particularly in software development. Coding assistants support code generation, debugging, code reviews, root cause analysis and maintaining documentation, which is delivering meaningful time savings on repetitive tasks and faster onboarding of technical staff. In turn, some banks report that early results have translated into significant cost savings in some cases. Beyond development functions, some financial institutions have also deployed organisation-wide GenAI assistants to support drafting, research and information retrieval across business functions. This has reportedly improved knowledge access and internal collaboration across the organisation.

Case study: Operational efficiency with AI adoption

A large internationally active insurer conducted a global review of manual workflows to identify where AI could have the most immediate and governable impact. This resulted in the elimination of approximately 400,000 manual processing instances in 2025.

One notable example that the insurer embarked on was the underwriting quick quote process. In this workflow, front line staff submit email enquiries to the underwriting team containing client information, which the team then analyses to prepare preliminary assessment documents. These assessments play a critical role in the sales process, helping producers narrow their insurer selection before proceeding to formal applications. With approximately 4,000 such requests received each month, the process involved significant time and manual work.

With the deployment of AI, upon receipt of a producer's email, the system now automatically analyses the client information and generates a draft preliminary assessment for underwriting team's review. This reduces turnaround time from one business day for simpler cases and two to three days for complex ones, to approximately 45 seconds.

The insurer is also adopting AI for software development to improve developer efficiency. This has increased productivity through leveraging AI code generation tool across the company to write six million lines of code in 2025, with around 80% adoption rate among developers.

Operational resilience

Several financial institutions are using AI to enhance operational and cyber resilience, such as threat detection and response. AI can analyse large volume of data in real time to identify anomalies and detect potential attacks faster than human analysts, while also reducing false positives, allowing for effective containment of threats. Furthermore, AI can strengthen organisational resilience by identifying vulnerabilities and can promote business continuity through swift recovery from incidents like ransomware attacks.[25]

Financial institutions of various sizes and types use AI to monitor anomalous network behaviour across internal employee access, data transfers and unusual API calls, using a combination of

[25] See G7 Cyber Expert Group (2025).

internal and third-party tools. AI can also be used to identify phishing attempts. GenAI can rapidly populate internal security alerts and incident reports.

Case study: Operational resilience with AI

A global electronic payment network operator used AI to enhance its payment resiliency by helping participating financial institutions maintain payment continuity during disruptions to payment processing. The highly distributed and interconnected nature of the payments ecosystem means disruptions at a single participant can have spillover effects on customers, merchants and the broader financial system.

To mitigate these risks, the network introduced a set of AI-enabled capabilities supporting authorisation decisioning, account information sharing and contingency management. During issuer outages that prevent financial institutions from processing payment authorisations through their normal systems, AI-supported decisioning can evaluate more than 200 transaction variables and make authorisation decisions on behalf of participating financial institutions. This allows payment processing to continue even when issuer systems are unavailable**,** with AI drawing on historical decision patterns to improve authorisation accuracy and reduce customer disruption. Participating financial institutions may also share account information, such as spending limits, to support more precise authorisation decisions and mitigate overdraft or over-credit-limit risks when operating under contingency arrangements. In addition, financial institutions can establish customised contingency parameters that are automatically activated when predefined disruption conditions are met.

1.3. Risks and implementation challenges of AI adoption for financial institutions

As noted in the FSB's 2024 report, four types of AI-related vulnerabilities stand out for their potential to increase financial stability risks:[26] (i) third-party dependencies and service provider concentration; (ii) market correlations; (iii) cyber risks; and (iv) model risk, data quality and governance. This report builds on the FSB's previous analysis of these risks and describes additional AI-related risks and implementation challenges that can impact financial institutions and their customers.

Inadequate governance and strategic execution

AI has the potential to rapidly transform a wide range of existing business processes, but inadequate governance and lack of board and senior management oversight can give rise to significant risks. Without clear accountability within the financial institution, critical issues may be overlooked. Inadequate assessments of the materiality[27] and risks of AI use cases can lead to mis-calibrated risk management. Particularly at large financial institutions, fragmented AI implementation across business units can undermine effective risk management. Governance gaps may also enable the use of 'shadow AI', where employees adopt, develop or deploy AI tools or applications without authorisation and for unapproved uses, reducing financial

[26] See FSB (2024b) Section 4.2.

[27] The materiality of an AI use case generally means the extent to which the AI model or system is used by the financial institution and how it might affect the organisation and its customers. Assessing materiality generally involves considering factors such as potential financial consequences, role in key decisions, involvement in compliance with laws or regulations, use with customers, scale of use throughout the organisation, reversibility of outcomes, and interaction with external parties and sources.

institutions' visibility of and ability to monitor and manage AI-related risks. Insufficient evidentiary controls, such as gaps in documentation, may also hinder the auditability of control effectiveness and accountability and traceability of decision processes, particularly for consequential decisions with material impact to financial institutions or their customers.

Ineffective data governance and poor data quality

Ineffective data governance and poor quality data can lead to a number of AI-related risks, including data compliance and security risks, model risk, unacceptable bias,[28] and poor AI performance. For example:

- AI models or systems can perpetuate or amplify biases and inaccuracies present in input data, creating unanticipated or undesirable outcomes. These outcomes can become self-reinforcing, as biased outcomes generate new data that influences future decisions, entrenching biased patterns over time.
- poor AI performance due to overfitting[29] or underfitting[30], an inability to address outlier situations, or even unintended legal and regulatory breaches.
- breaches of any jurisdictional legal and regulatory requirements regarding data or potential infringement of intellectual property from AI-generated content.

Explainability challenges

While explainability can also be a challenge in non-AI models and other quantitative approaches, AI adoption introduces additional challenges to explainability and transparency, particularly in complex, autonomous, or rapidly evolving AI models or systems where the basis for decisions may be difficult to understand, made with no or minimal human involvement, or shift over time in ways that are difficult to follow. These challenges include:

- assessing conceptual soundness;
- confirming compliance with requirements in law and regulation;
- distinguishing causality from correlation;
- assessing reliability and robustness;
- detecting bias, errors, or performance issues, including data drift and model drift;
- understanding changes in dynamically updating models or systems;

---

28 Not all statistical differences or biases are necessarily unacceptable. Whether a bias is acceptable depends on the intended use and applicable legal and regulatory requirements.

29 Where AI works well with training data but not with unseen data.

30 Where AI fails to capture complexity of training data.

- assessing data quality, especially with inaccessible datasets (such as proprietary datasets of third-party AI providers); and
- conducting validation or independent review.

Inadequate or degrading AI performance

Inadequate or degrading AI performance can lead to poor decision-making as well as financial, legal, regulatory, operational and other risks. The higher the materiality and risk of the AI use case, the greater the potential impact of performance issues, which can adversely affect the financial institution as well as customers and market participants. For example, models trained on historical data may underperform in new market conditions. Some type of AI such as GenAI may hallucinate by generating seemingly plausible but incorrect outputs. GenAI models may also overlook or underweight relevant information in lengthy or complex inputs, producing fluent and seemingly complete outputs based only on part of the information provided. Other models might execute inappropriate or harmful tasks. Performance may also degrade due to version changes in key AI models or systems and recovery and rollback can be challenging (or impossible) for some forms of AI models and systems.

Inadequate or inappropriate human oversight

Inadequate human oversight of AI may hinder financial institutions' ability to manage AI risks, causing unintended legal or regulatory breaches or customer harm, among other negative consequences. Certain misconceptions about AI can undermine the effectiveness of human oversight. Such misconceptions include the assumptions that AI always operates predictably in the same environment, that AI models or systems nearly always produce correct output, that the environment itself will remain predictable, or that human involvement ensures effective oversight. Human oversight may be weakened by over-reliance and/or automation bias.[31] Over time, sustained reliance on AI may also diminish staff expertise, judgement and challenge capability, which may in turn weaken effective human oversight and undermine fallback arrangements.

Cyber and ICT risks

The advent of AI has implications on cyber and ICT risks. For example, depending on where AI solutions are deployed within a financial institution, their use may have a bearing on system availability and data integrity, which can result from defective application codes generated by AI. In addition, the improper use of agentic AI could pose operational risks when the AI misunderstands a set of instructions due to unclear prompts and executes an automated task erroneously.

AI may also be weaponised and maliciously used by threat actors to attack financial institutions and their customers. This can result in an increase in the frequency and impact of fraud and cyber attacks.

---

[31] Overly trusting of automated systems outputs without critical thinking.

Examples of direct attacks against AI include:

- *Poisoning*: Threat actors inject biased or incorrect data into training data to manipulate model behaviour and outputs.
- *Malicious inputs* including:
  - *prompt injections*, where a threat actor manipulates prompts with malicious content to influence model behaviour and bypass safeguards.
  - *jailbreaking*: where a threat actor uses prompts to circumvent a GenAI model's safety features to breach legal requirements or guardrails. This can result in the model providing dangerous, illegal, or unauthorised outputs.
  - *evasion*: where malicious attackers make small, hard-to-detect changes [32] to input data to deceive an AI model, causing it to produce incorrect outputs.
  - *extraction*: where a threat actor reverse engineers an AI model to extract information about its architecture, parameters or training data.

Examples of AI-enabled attacks include:

- *Deepfakes and GenAI-enabled phishing*: the ability of multi-modal GenAI models to produce increasingly realistic audio, code, images, text and video can be used to amplify social engineering attacks through deepfakes, impersonation and false communications. Threat actors can, for example, impersonate individuals in a financial institution with authority to approve high-value transactions to defraud financial institutions or use AI-generated images or video to bypass KYC checks.[33]
- *Lower barriers to entry for other cyber attacks*: Advancements in AI models and AI-coding agents can allow threat actors to commit complex cyber attacks that previously required specialised technical capabilities. These advancements include developing malicious codes and identifying and exploiting severe security vulnerabilities at highly accelerated speeds (including zero-day vulnerabilities). Some advanced models can autonomously identify and exploit vulnerabilities through multiple means, including but not limited to source code analysis, web application testing, binary analysis and protocol fuzzing. They can also chain vulnerabilities together to amplify the speed and impact of attacks and reverse engineer patches developed to remediate known vulnerabilities. Such capabilities significantly compress the timeline from vulnerability discovery to exploitation.

Third-party dependencies and concentration

AI adoption in the financial sector increasingly depends on highly concentrated third-party providers across multiple layers of the AI supply chain, including cloud infrastructure, hardware,

---

[32] Examples include slightly modifying an image so that a security system misclassifies it, or tweaking text to bypass content filters using optimisation techniques and transferability.

[33] See MAS (2025b).

foundation models, data providers and deployment platforms. While third-party providers offer benefits, they also introduce risks. These risks apply not only to third-party AI tools and services, but also to those where third-party service providers incorporate or use AI within their tools and services not explicitly marketed or sold as AI (referred to as 'embedded AI'), including:

- Failure to perform as expected: Third-party AI systems may exhibit performance inconsistent with the terms of agreed-upon service.

- Insufficient transparency: Financial institutions may face reduced transparency when relying on proprietary or complex third-party AI models, systems, or data, limiting their ability to conduct due diligence, monitor performance and manage risks. For example, in the case of embedded AI, financial institutions may be unaware that their third-party tools or services incorporate or rely on AI. Third-party providers might also change the underlying models powering their AI systems without adequate notice, leaving financial institutions unaware of changes that could affect performance or risk outcomes. This can amplify explainability challenges of some forms of AI, such as GenAI and agentic AI.

- Data governance: AI models or systems provided by a third-party can pose risks if their training data includes inappropriate data, such as unlawfully processed personal data. Third-party AI systems may inadvertently disclose confidential or protected data. Third-party AI providers could also use financial institutions' data or customer data for unauthorised purposes.

- Operational resilience: Significant disruption to critical services provided by third parties can create risks for financial institutions' critical operations.

- Service provider concentration: Providers of cloud infrastructure, hardware, and AI foundation models are often highly concentrated and, in some cases, vertically integrated. Reliance on the same service provider for multiple critical services may magnify the impact of a disruption on individual financial institutions and create systemic third-party dependencies. Key parts of the AI supply chain, may also be geographically concentrated, increasing exposure to natural disasters and other supply chain disruptions.

- Homogeneous behaviours and correlated outcomes: Reliance on common AI models, datasets, or infrastructure can lead to correlated behaviours across financial institutions, amplifying risks like herding and procyclicality. This could exacerbate market stress, liquidity crunches and asset price vulnerabilities during periods of financial instability.

- Unclear contractual and legal liability: Financial institutions remain accountable for AI outcomes, even when they rely on third-party tools and services. However, contractual and legal liability for adverse outcomes - such as data breaches or negligence - is often unclear. This uncertainty may be particularly significant when third-party AI tools to generate, orchestrate, or execute actions by highly autonomous agents are used.

Consumer protection and market conduct risks[34]

Inadequate guardrails around AI could give rise to consumer harm and market conduct risks. This includes:

- Inadequate disclosure of AI use in financial services: Where there is insufficient disclosure about the role of AI in financial products and services, customers may be unable to fully understand or challenge decisions that affect them or seek appropriate redress.
- Unfair treatment and poor consumer outcomes: Use of AI models trained on biased or incomplete datasets may result in discriminatory results or outcomes not consistent with consumer protection requirements.
- Potential for mis-selling and unsuitable recommendations: The use of AI in customer-facing applications, including robo-advisory and product targeting, may lead to recommendations that are unsuitable or not aligned with customers' risk profiles, particularly where models rely on incomplete, outdated or improperly calibrated data.
- Reduced accountability and challenges in oversight of automated interactions: Increased reliance on AI-driven processes in marketing, advisory and customer engagement may blur lines of responsibility, making it more difficult for financial institutions and supervisors to identify, monitor and address misconduct or inappropriate practices in a timely manner.

Agentic AI risks

The high levels of autonomy that AI agents or agentic AI systems may have can create or amplify certain risks, which can materialise at great speed. Such agentic AI risks include:

- Unauthorised actions: AI agents may act autonomously in pursuit of pre-defined goals and, through interactions with their environment, may adapt how they pursue those goals. This creates a risk that they take illegal, unethical, or unauthorised actions without adequate human approval or oversight. In some cases, an agent may identify actions that appear to advance its assigned objectives, but are inconsistent with organisational policies, legal requirements, delegated authority, or other intended constraints. As the agent may treat these actions as effective shortcuts rather than recognise them as unauthorised, they can be difficult or impossible for humans to detect, override, or remediate.
- Erroneous actions: AI agents might make incorrect decisions due to goal misalignment, insufficient information, random errors, planning or execution errors, limitations in their ability to generalise to new circumstances, or other performance-related shortcomings. These actions may only manifest once the agent is deployed in a live environment. Monitoring and detecting these actions in real-time can be very difficult. An AI agent can take hundreds of intermediate steps in pursuit of its goals and make errors in any

[34] This section may also apply to protection of investors.

of those steps. In some cases, effective monitoring and detection may require augmentation with another AI agent or other forms of AI.

- Data security, data breaches and privacy risks: AI agents may expose or manipulate sensitive data such as customer details, trade secrets, or internal communications. This may happen through malicious attacks where threat actors exploit vulnerabilities of agents, accidental disclosure if agents fail to recognise data sensitivity, or autonomous actions that inadvertently lead to exposure of sensitive data such as customer details. In the absence of additional controls and guardrails, some agents with advanced capabilities may interact with datasets (internal or external) that they should not have access to.

- Disruption to connected systems: To execute complex tasks, AI agents can integrate with Application Programming Interfaces (APIs), databases, ICT systems and other agents, all of which can be disrupted if the agent is compromised or malfunctions. AI agents may also collude with other AI agents to carry out cyber attacks (e.g. deleting code or carrying out Distributed Denial-of-Service (DDoS) attacks) or other malicious actions, such as spreading disinformation, to achieve their goals. Even without collusion, multiple AI agents may interact in unanticipated ways that create unforeseen behaviours or risks.

- Additional risks from inadequate human oversight: AI agents pose a distinct challenge for human oversight, given the impracticality of real-time human monitoring of agent decisions as their use scales. This challenge is further compounded in live environments, where opportunities for human intervention may be limited once actions are being taken. This can also lead to agents pursuing objectives or taking actions that deviate from the financial institution's intentions or risk appetite, without staff being aware or able to intervene in a timely manner.

- Additional cyber and ICT risks that pose challenges for traditional cyber security controls: For example, threat actors can manipulate AI agents by injecting malicious data into their knowledge base (known as memory poisoning), influencing their behaviour over time.[35] Agents may also devise novel ways to evade traditional cyber detection capabilities.

- Sub-agents and agent orchestration: Some AI agents can spawn and orchestrate sub-agents to carry out specific, delegated tasks in pursuit of their predefined goals. The resulting dispersion of decision-making and execution across multiple agents can: weaken the effectiveness of governance, oversight and control mechanisms; increase the risk of unauthorised or unintended actions; and amplify the risks referred to above.

[35] Malicious data can be injected to AI agent's retrieval-augmented generation (RAG) to manipulate its learning and memory process known as agentic memory poisoning.

2. Organisation-wide AI governance

The four sound practices in this section address AI governance practices at an organisational level and the eight sound practices in the next section cover the AI lifecycle. As is the case with cross-sectoral standards on AI,[36] these four sound practices are designed to be cross-cutting to inform the remaining sound practices.

AI governance concerns how financial institutions choose, monitor and review their approach to AI adoption and organisational governance. As in other areas, the board and senior management[37] take responsibility and play critical roles in setting a clear direction for AI adoption and in providing senior-level oversight, so that AI adoption and governance align with the financial institution's business model, risk appetite and strategy (Sound Practice 1). The board and senior management are also responsible for establishing and maintaining clear and well-defined roles and responsibilities across the organisation, to promote effective accountability and robust oversight of AI-related activities and risks (Sound Practices 2 and 3). Financial institutions adapt their governance approaches and operating models and appropriately resource the organisation as AI and the financial institution's usage evolves (Sound Practice 4).

2.1. Strategic direction and oversight

> **Sound Practice 1 (Strategic direction and oversight):** The board and senior management align AI adoption and governance with the financial institution's business model, risk appetite and strategy.

The board and senior management oversee AI adoption

The board and senior management consider AI adoption as part of the financial institution's business strategy. This includes considering how AI may positively impact the financial institution's business model, risk management, customers, efficiency, growth and compliance with legal and regulatory requirements, while balancing these benefits against AI-related risks. As in other areas, the board promotes clear accountability for senior management to implement the financial institution's approach to AI adoption.

Financial institutions may incorporate relevant roles and responsibilities into existing governance and management roles and may engage external experts to inform and support the board and senior management in their oversight of AI adoption. This approach may particularly benefit smaller financial institutions.

---

36 For example, NIST AI Risk Management Framework. See NIST (2023).

37 This report refers to a management structure composed of a board of directors and senior management. There are significant differences in legislative and regulatory frameworks across jurisdictions regarding the functions of the board of directors and senior management. In some jurisdictions, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) and is known as a supervisory board. This means that the board has no executive functions. In other jurisdictions, the board has a broader competence in that it lays down the general framework for the management of the organisation. The terms 'board of directors' and 'senior management' are used in this report to label distinct decision-making functions within a financial institution.

The board and senior management define and communicate across the organisation the outcomes expected from AI adoption, including the desired outcomes from appropriate risk management. This fosters alignment between the financial institution's business strategy and its approach to and execution of AI adoption over time. The board and senior management are engaged end-to-end, from strategy through implementation, so that processes (e.g. governance of AI outputs used in decision-making) and resources (e.g. organisational capabilities, investments in technology infrastructure, strategic partnerships) are aligned with the intended outcome.

The board and senior management regularly re-assess whether the financial institution's approach to AI adoption remains fit for purpose. A reassessment may also be triggered by material changes in technology, the financial institution's maturity in AI adoption, or significant changes in the risk landscape. The board receives and considers management information (MI)[38] that allows it to assess whether the financial institution's approach to AI adoption, including previous decisions not to adopt AI for certain use cases, remains aligned to its strategy and risk appetite; complies with legal and regulatory requirements; and is being implemented effectively by senior management.

The board and senior management consider AI risks when setting risk appetite and tolerance

The board and senior management establish clear boundaries for AI adoption by considering AI risks when setting and reviewing the financial institution's risk appetite and tolerance.[39] These boundaries could include criteria for adopting high-risk and/or high-materiality use cases, as well as prohibitions on specific uses, for example, fully automated decision-making in critical business areas where the assessed risks exceed the financial institution's risk appetite or tolerance. In setting these boundaries, the board and senior management consider different types of AI and potential AI use cases: the level of explainability and transparency; extent of autonomy; materiality and risk; potential customer impact; legal and regulatory requirements; and dependencies on data, technology and third parties.

The board and senior management also align AI adoption with the financial institution's standards for conduct. This considers impact to customers and markets and informs their decisions on explainability, human oversight and redress for specific AI use cases.

The financial institution's risk appetite and tolerance guide decisions on AI use, selection and prioritisation, as well as the controls needed to monitor, manage and mitigate associated risks. These controls may include effective oversight, evidence of governance and control - particularly for highly autonomous AI - and clear escalation protocols. This becomes particularly important as AI adoption expands to critical operations and core business lines. Addressing AI considerations explicitly in the financial institution's risk appetite helps align board-level oversight and management action.

---

[38] As with other areas, MI include: business plans; risk reports (including high-risk uses); performance reports; failures and mitigation actions; and audit reports. MI may also include metrics on AI adoption, such as time savings (in some cases with estimated monetary value), utilisation/uptake by staff, customer satisfaction, and acquisition measures.

[39] Risk appetite is defined as the aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan (see FSB (2013)). Meanwhile, risk tolerance can be defined as the boundaries of specific risks that financial institution can take or withstand.

The board and senior management appropriately resource the financial institution to support AI adoption

The board and senior management appropriately resource the financial institution to support AI adoption currently and on an ongoing basis. This includes ensuring that the board, senior management and staff - including those in control functions - have the competencies and skills to fulfil their respective roles and responsibilities. It also includes maintaining sufficiently mature data and technology capabilities to support sustainable AI adoption. The board and senior management regularly reassess the adequacy of these resources, skills and capabilities as AI becomes more embedded in critical operations and core business lines and as technology and applicable legal and regulatory requirements evolve.

Case study: Aligning skills and capabilities to AI strategy

Some large internationally active financial groups, under the steer of their boards, treat AI as a strategic pillar rather than as a mere technological tool. These financial institutions have pursued end-to-end redesign of processes and workflows across their organisation, with AI fundamentally shaping how those processes are structured and operate. To support this, the board and senior management of these financial institutions have invested in building capabilities at all levels of the organisation. Senior managers and board members have undertaken master classes developed with reputable academic institutions and management consultants to build the transformative mindset needed to drive such change, while staff have been supported through AI bootcamps to become 'hybrid' professionals combining domain expertise with AI development skills, alongside organisation-wide programmes to build AI literacy.

These financial institutions have also set concrete targets to track AI adoption progress, covering both hard benefits such as productivity and cost metrics and softer benefits such as enhancements to staff capacity. They have acknowledged, however, that finding suitable metrics remains challenging, particularly around value realisation.

Other financial institutions have focused instead on layering AI onto existing processes to improve services and enhance productivity, without pursuing broader organisational transformation. For these financial institutions, board and senior management have correspondingly focused on building AI literacy across the organisation and implementing clear boundaries around AI use, such as restricting staff to specified tools accessed only through prescribed platforms. This approach seeks to enable staff to work effectively with AI tools within their existing roles and workflows.

2.2. Governance and accountability

Sound Practice 2 (Governance and accountability): Financial institutions define clear roles and responsibilities and maintain an appropriate governance framework to enable responsible AI adoption.

Define clear roles and responsibilities

Financial institutions define clear roles and responsibilities for AI adoption, building on existing structures such as the three lines of defence[40] or by creating new structures, if appropriate. For

[40] See BCBS (2021b). The three lines of defence commonly consists of business unit management, an independent corporate operational risk management function, and independent assurance. Depending on the organisation's nature, size and

example, under the three lines of defence model, first-line functions assess business outcomes, controls, materiality and risks for AI use cases. The board and senior management may designate specific first-line function executives as accountable for high-materiality and/or high-risk AI use cases and their outcomes. Second-line functions maintain an organisation-wide view of AI-related risks across the financial institution and independently assess or validate first-line activities. Their review may cover compliance, data quality, explainability, conduct risk, cyber and ICT risk and model performance. Finally, third-line functions deliver assurance proportionate to the materiality and risk levels of the AI use cases.

Control functions - including audit, evaluation, risk management and testing - remain objective, unbiased and functionally separate from development teams and business users. Staff performing these functions are empowered and sufficiently skilled to provide effective challenge. Where AI is used to monitor and manage the performance and risks of another AI model or system, the monitoring AI is independent of the AI model or system under review.

Maintain an appropriate operating model for responsible AI adoption

Financial institutions' operating models consider the nature and scale of AI adoption within the organisation. The operating model may be centralised, decentralised, or a hybrid of both. Centralised models offer consistent oversight and standards across all AI use cases. Decentralised approaches provide business units and functions greater flexibility and the ability to leverage domain-specific expertise. Hybrid models combine elements of both. Financial institutions may choose to adapt and leverage existing operating models. The operating model is reviewed regularly, and following material changes in AI adoption, technology or the risk environment. These reviews help ensure that: the financial institution's strategy remains effective; risks are assessed and managed consistently across the organisation; and AI adoption remains aligned with the financial institution's risk appetite and tolerance.

Case study: Integrating AI governance into existing risk management framework

A G-SIB with significant capital markets and broker-dealer activities adopted AI-specific governance practices by embedding them within its established organisation-wide risk and control frameworks, rather than building a separate governance structure for AI. The bank recognised that many risks arising from AI, GenAI and emerging agentic AI capabilities were already addressed through mature enterprise disciplines - including technology, risk and compliance, data and legal - and concluded that AI-specific risk management generally required targeted enhancements to these frameworks rather than wholly separate ones. Formal risk and control committees continued to oversee each of these disciplines.

To provide organisation-wide visibility, the bank established a dedicated AI governance committee that is chaired by a senior executive. The committee identifies governance and control requirements and monitors emerging risks and control issues. Its charter defines its scope, membership and meeting frequency, as well as a clear channel for escalating issues to the relevant risk committee. To connect organisation-wide oversight with day-to-day activity, each business and functional area maintains its own AI governance body, with an escalation path to the central committee. Each area also designates an AI governance lead responsible for implementing the framework and representing the area at the central level. This cross-organisational model enables AI-specific risks to be identified and governed with appropriate expertise, while avoiding fragmented or duplicative controls. Governance expectations

complexity, and the risk profile of an organisation's activities, the degree of formality of how these three lines of defence are implemented will vary.

were calibrated proportionately to the risk of each case and capabilities of the technology, so that heightened controls apply to higher risk uses (such as those directly affecting customers or regulated decisions or involving GenAI and autonomous AI technologies) rather than to tools with a lower risk profile.

Establish cross-functional coordination mechanisms

Financial institutions implement cross-functional coordination mechanisms to leverage on the diverse perspective from business owners, risk managers, technology experts, compliance officers, legal specialists, developers and other relevant stakeholders. This facilitates knowledge sharing and supports balanced decision-making when stakeholders across the financial institution understand and manage the full range of benefits and risks of AI, optimise implementation plans and clearly delineate responsibilities and accountabilities. Cross-functional coordination mechanisms may include regular fora; standardised communication channels; consistent methodologies for assessing, monitoring and reporting AI risks; and feedback loops that adapt governance and risk frameworks to evolving AI risks. Cross-functional coordination can also support end-to-end assessment of highly autonomous AI, including interactions and dependencies amongst different models, systems and agents, to identify risks and mitigate them.

2.3. AI risk management framework and effective documentation

Sound Practice 3 (Incorporation of AI risks into risk management framework and effective documentation of AI use): Financial institutions adopt risk management frameworks that effectively address AI risks and include processes for documentation of AI use, as well as for materiality and risk assessment.

Consider relevant risks from AI in risk management frameworks

Financial institutions incorporate AI risk considerations into existing risk management frameworks, policies and procedures, as appropriate. This allows AI risks to be identified, assessed, accepted (or approved), documented, monitored and managed. Section 3 describes AI lifecycle management frameworks relevant to AI adoption in more detail.

Where existing policies, procedures and frameworks do not sufficiently address AI risks, such as those related to lack of transparency, lack of explainability, autonomy, or inadequate or inappropriate human oversight, financial institutions enhance these policies, procedures, or frameworks, or establish new ones as appropriate.

Financial institutions implement guardrails and controls proportionate to materiality and risks (e.g. streamlined processes for low materiality and low risk use cases and rigorous processes for high-materiality and/or high-risk use cases). Guardrails implemented at the different stages of the AI lifecycle can also vary by use case (see Section 3). They may include staged approvals, comprising supervised experimentation in controlled environments and pilot phases before deployment.

Maintain accurate documentation and lifecycle records of AI use

To maintain visibility over risks from AI adoption and facilitate effective identification, assessment, monitoring and management of AI risks in a proportionate manner, financial institutions maintain appropriate documentation and lifecycle records of their AI use throughout their lifecycle.[41] Documentation describes the AI use case, including its purpose, design, governance arrangements, risk assessments, approvals and key lifecycle decisions.[42] Lifecycle records, including logs and other records generated through development, deployment, operation, monitoring and incident management activities, capture key information of the AI use case across its lifecycle. Together, documentation and lifecycle records support accountability, verification, assurance and auditability. Financial institutions leverage existing processes and repositories, such as use case and model inventories, third-party registries, or systems registry. Financial institutions may have more detailed documentation and lifecycle records for higher materiality and higher risk AI use cases.

Documentation and lifecycle records captured can include:

- a description of the AI use case, such as:
  - (i) its underlying AI model(s) or system(s) and the rationale for its selection;
  - (ii) approved, intended or prohibited applications; and
  - (iii) whether it was developed in-house, uses open-source tools, or was acquired from a third-party AI provider.
- materiality and risk of the AI use case and mitigants.
- business lines, regions, products, customers and market participants impacted.
- key assumptions and limitations about the AI use.
- data sources used during inference and, if developed in-house, data used for training.
- allocation of accountability (i.e. owner of the AI use case and other key roles and responsibilities) at the financial institution.
- dependencies on other AI uses, models, systems, critical data sources, third-party AI providers, cloud services, or fallback arrangements.
- AI lifecycle stages and status.
- findings from testing, ongoing monitoring and performance assessment.[43]

---

41 Proactive record-keeping from inception promotes effective AI risk management.

42 Documentation may not involve documenting every single AI use case to the extent described, especially those that are much less material.

43 For example, indicators of whether AI models or systems are functioning properly, the dates when those indicators were last updated, and any outstanding remediation actions.

- information related to validation or independent review.
- relevant information from third-party AI providers.[44]

Financial institutions protect documentation and lifecycle records from unauthorised manipulation (modification or deletion) and, if possible, make them immutable or keep immutable copies especially if they contain critical information.

Consider additional aspects for GenAI and agentic AI

Financial institutions retain sufficient records throughout the AI lifecycle to document actions, decisions, recommendations and outputs made by, or with the assistance of AI. These records support auditability, verifiability, assurance and effective risk management. They may include prompt versioning[45] and version control to enable rollback to previous configurations, as well as model parameters and performance records to identify changes over time and chain-of-thought logging to help explain outputs.

In the case of agentic AI, financial institutions establish effective record-keeping to enable them to: attribute actions (decisions, intermediate steps, escalation to a human, interactions with the external environment etc.) to specific agents; assess these actions; and promptly identify and manage anomalous or risky behaviour. This facilitates human oversight, ongoing monitoring and the detection of unusual activity. Attribution encompasses visibility and traceability.

- Visibility assigns individual unique identifiers to each AI agent so that financial institutions can see which actions it took and which humans configured and oversaw it. Unique identifiers for agents allow them to be easily differentiated from human users and other ICT systems.
- Traceability allows financial institutions to follow what a given AI agent did, including: what triggered the action; what information and tools it accessed; what steps it took; and whether it acted within its permissions throughout this chain of steps.

As financial institutions scale up their use of agentic AI, they take a risk-based approach to the amount of information they log to focus on actions, decisions and steps that can impact their risk profile without collecting and retaining unnecessary and potentially unmanageable volumes of data.

Case study: Documentation of AI use cases

Some large internationally active banks maintain a centralised, organisation-wide AI inventory supported by dedicated software systems, giving them clear visibility over their AI footprint and the risks arising from it. These systems serve as a repository for comprehensive documentation of individual AI use cases, with records maintained throughout the AI's lifecycle. Key attributes captured may include the AI's purpose, scope of use, risk materiality rating, dependencies, responsible personnel and approvals obtained, among others. Beyond recording where AI is used, these systems may also support features such as automated tracking of approvals and issues, identification of interdependencies between models and lifecycle tracking with checkpoints at key risk management stages. Some other

[44] For example, acceptable use policy; model or system cards; certifications, standards and other assurance; or any customisation or fine-tuning by the financial institution.

[45] The systematic practice of tracking, management, and auditing of AI prompt iterations.

banks with more limited AI adoption to date have been observed to rely on spreadsheets for their AI inventories.

Where banks deploy agentic AI systems, additional attributes beyond those captured for standard AI models have been included in their inventories. These include agentic AI-specific identifiers, the tools the agent can access, its components and guardrails to manage risk. Where banks have adopted a modular approach - with reusable agents deployed across multiple use cases - some banks have tracked risk information at the agent level, including permitted uses and known risks of each agent, rather than solely at the use case level. In more mature organisations, this has taken the form of agent 'certification', where an agent is reviewed and approved for use within defined boundaries - with its certified status and permitted scope recorded as inventory attributes. As governance practices for agentic AI are still rapidly evolving, the attributes captured for such systems are expected to develop further as industry norms and regulatory expectations mature.

2.4. Organisational adaptability

Sound Practice 4 (Organisational adaptability): Financial institutions learn, adapt and adjust their oversight, governance, risk management practices and capabilities as AI evolves.

Sustain AI expertise and risk-aware culture

Financial institutions develop and maintain AI expertise and embed a risk-aware culture that encourages challenge, escalation and continuous learning. Organisational adaptability is only possible with adequate capability across the financial institution - from foundational literacy for all staff to specialised expertise for implementers and risk managers and informed board and senior management oversight.[46] Capability-building efforts specific to AI may include:

- providing foundational AI training for all staff so that they can recognise and respond to inappropriate use, automation errors, automation bias/over-reliance and unusual model behaviour;
- developing role-specific expertise for developers, validators, risk managers, auditors and compliance teams to manage AI-specific risks (e.g. data/model drift, instability, unusual AI behaviour, explainability gaps, data vulnerabilities);
- maintaining human expertise and critical judgement by preserving opportunities for staff to exercise decision-making, challenge AI outputs, develop domain knowledge and retain the skills necessary to operate effectively when AI tools are unavailable, degraded, or produce incorrect or misleading outputs;
- offering targeted oversight training for the board and senior management to enable them to identify and make informed decisions on AI-related risks and opportunities;

[46] See The MindForge Consortium (2026), pp.109.

- embedding a strong risk-aware culture that encourages detection of emerging risks, early escalation, questioning of model outputs and consistent application of governance across business lines; and

- integrating insights from incidents, data/model drift events, near-misses, testing outcomes and validation findings, as well as relevant information from third-party AI providers, into staff training and behavioural expectations to align capabilities with operational experience.

Maintain external awareness

Financial institutions proactively monitor developments outside the organisation for timely awareness of new technology, risks and supervisory expectations. External developments can surface early risk signals that internal processes may not yet detect. Such efforts to maintain external awareness specific to AI can include:

- monitoring emerging AI capabilities, model architectures and risk typologies to detect external shifts that may impact internal risk assessments;

- engaging regularly with peer financial institutions, industry groups, academics, technology providers and authorities to remain informed about industry developments as well as any relevant regulatory and supervisory initiatives;

- participating in shared-learning fora, collaborative testing and public-private consortia to identify risks or practices observed across the financial sector and share relevant information (e.g. on risks, vulnerabilities and remediation); and

- establishing processes to analyse external intelligence and flag potential areas requiring governance review.

Case study: Learning from the AI ecosystem through public-private sector collaboration

Several authorities have established structured public-private sector collaboration platforms - including industry consortia and regulatory sandboxes - to build shared understanding of AI opportunities and risks. These platforms bring together authorities, financial institutions and technology partners to develop practical guidance and deepen supervisory insight.

For example, the Monetary Authority of Singapore (MAS) convened Project MindForge in 2023, bringing together financial institutions, industry associations, technology partners, as well as consulting and technology partners to examine AI risks and develop practical guidance.[47] The consortium produced a whitepaper on the emerging risks and opportunities of GenAI for banks in November 2023 and subsequently an AI Risk Management Toolkit to support financial institutions in implementing AI risk management practices in March 2026. Similarly, the Bank of England (BOE) and Financial Conduct Authority (FCA) established the AI Consortium in May 2025 to gather input from stakeholders on the capabilities, development, deployment and use of AI in UK financial services.[48] The AI Consortium aims to identify how AI is being used in financial services, discuss emerging benefits and risks and inform their approach to safe AI adoption.

---

47 See MAS website.

48 See BoE website.

Other authorities have used regulatory sandboxes to enable financial institutions to pilot AI use cases in a controlled environment. Launched in 2024, the Hong Kong Monetary Authority (HKMA)'s GenAI Sandbox provided participating banks with supervisory guidance, technical support and access to Graphic Processing Units (GPU) computing resources, while industry symposia and roundtables facilitated broader knowledge sharing. Building on its success, the GenAI Sandbox has since expanded to cover multiple financial sectors including banking, securities and capital markets, asset and wealth management, insurance, mandatory provident fund and stored valued facilities.[49]

Evolve with insight

Financial institutions update governance, controls and oversight mechanisms as needed, based on lessons learned from both internal and external insights, such as AI incidents, testing outcomes and emerging risks. These updates can include:

- reviewing governance, lifecycle controls and oversight roles as risks evolve;
- reassessing internal assumptions, including due to external developments to avoid outdated mental models or blind spots;
- performing root-cause analysis and post-incident reviews for AI-related incidents, recognising that AI incidents may reflect underlying issues that traditional analysis and reviews may not always be designed to capture (e.g. societal biases in training data);
- treating relevant anomalies, drift events and near-misses as triggers to assess and, where needed refine controls, given AI models' unique and non-linear degradation patterns;
- refreshing policies, standards and procedures based on learning and maintain governance as internal experience accumulates;
- implementing governance mechanisms so that they adapt to new forms of AI (e.g. GenAI, foundation and frontier models, agentic systems) that introduce new risks; and
- incorporating lessons learned into capability development and tooling enhancements, strengthening the financial institution's ability to respond to future issues.

Case study: How an adaptive AI strategy delivered industry leadership

A G-SIB's AI approach has evolved through distinct phases, adapting governance, operating models and controls as AI moved from experimental use to core business infrastructure.

The bank started by investing in internal research capabilities, specialised technical talent and proprietary data infrastructure. This research-first approach enabled the bank to develop institution-specific AI methods suited to complex financial decision making, while also building a substantial portfolio of AI-related intellectual property. After about a year, the bank shifted from research to implementation in areas where AI seemed to be most fruitful and governable. These early deployments demonstrated that advanced AI systems could operate reliably and deliver measurable outcomes without undermining risk controls. In parallel, the bank invested in enterprise grade data and computing

[49] See HKMA (2026).

infrastructure to enable secure development and deployment at scale. AI capabilities were progressively embedded into internal tools used by tens of thousands of employees, including productivity, research and software development functions. As AI adoption expanded over a couple years, the bank identified the limitations of decentralised development and adapted its organisational approach, by creating a centralised AI group reporting directly to the Chief Executive Officer. This group now functions as an enterprise accelerator, responsible for prioritising use cases, coordinating deployment across business lines and ensuring consistent application of risk, security and compliance standards.

This structural change marked a transition from project-based experimentation to industrial scale AI delivery. The new approach embeds privacy, security, fairness, accountability and transparency requirements across the AI development and deployment stages - from design and training to monitoring and audit.

3. AI lifecycle management

This section focuses on sound practices related to the management and mitigation of AI risks throughout the stages of AI development and deployment or 'AI lifecycle', which is explained in Section 3.1. Sound Practices 5-10 relate to certain stages of AI development and deployment, while Sound Practices 11 and 12 relate to cyber and ICT risk management as well as third-party risk management that apply across all stages.

3.1. Stages of AI development and deployment

Regardless of the term used, it is important to note there are no standard, one-size-fits-all stages of AI lifecycle. Different AI use cases may involve different stages of development and deployment of varying length.

In this report, the following illustrative AI lifecycle with seven distinct stages is provided to help financial institutions manage AI risks and adopt the relevant sound practices.[50] The seven stages of AI development and deployment in this report include:

- **Inception**: Identifying the needs, goals and feasibility of the AI use case. This stage involves defining the context, potential use case(s), materiality and risk assessment.
- **Design and development**: Defining the system architecture, data flows, selecting the AI model or system and security assessments, in line with secure-by-design principles (see also Sound Practice 11). Key activities include data governance, component selection and implementation of initial safety controls. If applicable, this stage may also include training an AI model, or customising or fine-tuning of third-party or open source AI models or systems.

[50] Financial institutions may develop their own AI lifecycle management processes with their choice of stages or adopt the lifecycle stages of different regulation, guidance and standards. For example, NIST AI Risk Management Framework uses a four-stage lifecycle (plan, design, develop, and deploy). For details, see NIST (2023).

- **Verification and validation**: Testing[51] and confirming that the AI use case meets specified requirements (verification) and performs as intended in real-world scenarios (validation).
- **Deployment**: Releasing the AI model or system into its operational environment, which includes setting up human oversight and monitoring.
- **Operation and monitoring**: Running the AI model or system, logging activity and monitoring for performance, safety and security risks (including data drift).
- **Re-evaluation**: Periodically assessing whether the AI use case continues to meet its objectives under changing conditions, which may lead to retraining or updating.
- **Retirement**: Decommissioning the AI model or system as well as addressing long-term data and access risks, such as archiving or data disposal.

3.2. Materiality and risk assessment

> **Sound Practice 5 (Materiality and risk assessment)**: Financial institutions implement an effective and systematic approach to assess the materiality and risk of AI use cases at the inception stage and thereafter.

Assess materiality and risks of AI use cases at the inception stage and thereafter

The materiality and risk profile of an AI use case are interrelated but different concepts. In practice, financial institutions may assess them within a single process. Both materiality and risk are relevant in deciding the appropriate and proportionate level of risk management and risk mitigation for an AI use case, including guardrails and level of human oversight.

The materiality of an AI use case refers to its importance to the financial institution's viability, 'critical operations',[52] and its ability to meet key legal and regulatory obligations (including towards customers). The materiality assessment of an AI use case typically considers the criticality of the operations or business lines supported by the AI use case and the importance of the AI use case to those business lines or operations. On the latter, an AI use case may support critical operations or core business lines in various ways, ranging from narrow administrative tasks (e.g. automated document sorting) to being essential to their effective functioning. Consistent with other FSB publications,[53] when assessing materiality, financial institutions consider:

- Importance: the financial, operational, or strategic importance of the AI use case to the financial institution, including to any critical operations or core business lines that rely on it.

---

51 Testing includes adversarial testing, where appropriate.

52 See FSB (2024a) and BCBS (2021a), pp.3. Some jurisdictions use different terminology, such as 'important business services' or 'critical or important functions'.

53 See FSB (2023b)

- Tolerance for disruption: the applicable tolerance for disruption to the operations or business lines supported by the AI use case, whether set by the financial institution, financial authorities or SSBs.

- Data: the nature of any data or information used which the AI model or system will be trained on or, if applicable, be able to access to deliver its outputs to achieve pre-defined goals. This may include data used by or shared with a service provider.

- Substitutability: or lack thereof, of the AI model(s), system(s) underpinning the AI use case (and, if applicable, the service provider(s)). This includes the availability and costs of models or systems with equivalent capabilities.

The materiality of an AI use case may change over time. Financial institutions often deploy AI use cases in non-critical operations and business lines initially and scale to critical operations progressively as they gain comfort with use. Therefore, in addition to assessing the materiality of a proposed AI use case at inception, financial institutions reassess it at regular intervals and upon certain events or milestones (e.g. a decision to scale up the use of the AI use case to critical operations).

The risks of an AI use case refer to the potential harm it may cause to the financial institution or its customers. A use case can pose high risks even if it is not material. For example, a highly autonomous AI agent performing a low materiality task (or operating in a contained training environment) could cause significant harm if it acts outside defined boundaries or escapes that environment.

Financial institutions systemically assess risks that an AI use case may create or amplify, including as a result of:

- the AI's autonomy, capabilities, complexity, the extent of access to systems and sensitive data and scope of action;[54]

- cyber/ICT vulnerabilities, data dependencies, explainability, reliability, substitutability, susceptibility to performance degradation and/or third-party/supply chain dependencies;

- the feasibility of human oversight and level of reliance on the AI use case's outputs; and

- relevant legal and regulatory requirements.

For each AI use case, financial institutions assess both inherent risk (i.e. the risk posed before relevant risk management and mitigation is applied) and residual risk (i.e. the leftover risk after risk management and mitigation is put in place).

As with materiality assessments, financial institutions take a dynamic approach to the risk assessment of AI use cases. Given rapid advances in technology and AI adoption, the AI risk

[54] This may include the financial institution's evolving understanding of what the AI is capable of doing and allowed to do. There are examples of AI agents, models, or systems being capable of performing actions they were not initially designed or expected to do.

landscape can change quickly. In addition to assessing the risks of a potential AI use case at inception, financial institutions generally repeat risk assessments periodically or upon the occurrence of certain events (e.g. after detecting incidents or performance degradation). Such reassessments can lead to risks being given a higher or lower tiering.[55]

In assessing the materiality and risk of their AI use cases, financial institutions can develop a specific framework or build on the work of the SSBs as well as financial authorities' respective regulations or guidance on AI risk management, model risk management,[56] operational resilience,[57] and third-party risk management.[58] In the latter case, financial institutions adapt and enhance relevant frameworks[59] to take account of AI-specific considerations and risks. Criteria used in existing frameworks can be directly relevant to assessing the materiality and risks of AI use cases (e.g. the complexity of the underlying AI model or system, criticality to operations,[60] or the nature of the data or information that the financial institution shares with third-party service providers). Regardless of the approach used, it is important to capture all relevant dimensions of materiality and risk systematically.

Consider additional aspects for agentic AI

Financial institutions consider the level of autonomy of an agentic AI system, its access to their data and systems and its ability to interact with the external environment when assessing its risk.

Financial institutions understand that the autonomy and capability of agentic AI is a spectrum ranging from agents performing administrative tasks to highly autonomous agents capable of executing entire, complex multi-step workflows. Financial institutions recognise that not every AI agent requires the same autonomy and access to achieve its goals and agree to a risk tolerance for each agentic AI use case at inception, which informs how much autonomy and access they grant to agents.

The risks associated with an agent's access to tools and systems may compound multiplicatively (rather than additively) as its permissions expand. When considering whether to extend an agent's autonomy or access (e.g. its ability to call on new tools, access data), financial institutions therefore consider the combined risks of the agent's new and existing access, rather than evaluate the new access in isolation.

3.3. Selection process

> **Sound Practice 6 (Selection process):** When selecting AI models or systems, financial institutions consider business objectives, operational and technical needs, as well as the materiality and risks of AI use cases.

---

55 For example, risks relating to the complexity of an AI model or system can reduce over time as both technology and its adoption mature, and these risks become better understood and managed or mitigated.

56 For example, see BOE/PRA (2023), ECB (2025), JFSA (2021), OSFI (2025b), and FRB et al (2026).

57 For example, see BOE/PRA et al (2021).

58 For example, see BOE/PRA (2021) and FRB et al (2023).

59 Existing frameworks include model risk management, operational resilience and/or third-party risk.

60 See FSB (2024a) and BCBS (2021a), pp.3.

Financial institutions have the ultimate choice of whether to adopt AI for specific use cases, taking into account alignment to their business strategy and their assessment of potential benefits and risks.

If a financial institution chooses to adopt AI for a given use case, during the selection stage it decides:

- whether to develop AI in-house, procure it from third-party AI providers, use open-source or open-weight tools, or use a combination of these; and
- the appropriate AI model or system (such as traditional, GenAI, agentic, or other emerging models or system, or a combination thereof) for the use case.

In making these decisions, financial institutions consider factors such as:

- materiality and risks;
- customer impact;
- intended use;
- whether the AI use case will apply across the financial institution, or to a specific business line or function;
- infrastructure and technical requirements;
- data needs and availability;
- readiness of the financial institution, including expertise and skills;
- legal and regulatory requirements;
- available resources;
- costs; and
- if applicable, third-party dependencies, risks and other factors (e.g. costs and permitted conditions of use).

Certain considerations may involve trade-offs. For example, high performing AI models or systems can be more complex, computationally intensive, costly and have less explainability or transparency than simpler AI models or systems with lower performance. The most complex AI models or systems may not invariably be the most appropriate. In some instances, a simpler, less costly, more explainable model or system may still deliver the financial institution's business needs.

Financial institutions assess the total cost of different AI models or systems, including commercial, computing, energy, financial and staffing costs. They also consider the potential for usage costs to rise rapidly as AI adoption scales, together with the costs associated with business continuity and contingency planning with third-party AI providers. Financial institutions consider ways to improve cost efficiency. The selection process is informed by research into the

capabilities of available AI models and systems, relevant industry practices and inputs from business users, control functions, subject matter experts and technical experts.

Once an AI model or system is selected, financial institutions implement appropriate, documented change management processes throughout the AI lifecycle, in particular, for high-materiality and/or risk use cases.

3.4. Data governance

> **Sound Practice 7 (Data governance):** Financial institutions establish appropriate data governance to maintain data that is fit-for purpose for training, testing and using AI (i.e. accurate, complete, consistent, reliable, secure).

Effective data governance is essential for effective AI risk management and for promoting high-quality data to underpin effective and reliable AI outputs.

Data governance and data quality are key regardless of whether a financial institution develops an AI model or system in-house using its own data, or relies on an AI model, system and/or data from third parties. However, in the latter case, there may contractual, legal, or practical limitations on the financial institution's ability to access or process third-party data. In such cases, financial institutions consider alternative or compensating ways to deliver the overall outcomes of ensuring sound data governance and high-quality data, including by assessing the third-party service providers' data governance practices, processes and data quality controls.

AI-specific considerations in data governance, which can apply to all types of data usage, include:

- the role of data in shaping AI design choices and outputs of AI, depending on the specific AI technology and use cases;
- the variety of data that are used in different AI applications, which may include multimodal (audio, text, image, video), unconventional (social media feeds) and synthetic data;
- the forms that data used by AI can take (structured, semi-structured, unstructured);
- the location(s) of the data, cross-border data transfers and jurisdictional requirements on the use of data in AI models or systems;
- the speed at which some data used by AI are generated and processed (velocity), which can be real-time or near real-time (e.g. for financial trading data and social media feeds);
- the volume of data used by, in particular, GenAI and agentic AI; and
- the ability of data to influence the behaviour (as well as outputs) of AI agents which creates additional risks around how agents ingest, interpret, memorise, use and re-use data.

Establish effective data governance frameworks

Financial institutions adopt a centralised data governance framework, decentralised but consistent frameworks, or a hybrid framework. This framework or frameworks may be pre-existing and cover the financial institution's approach to data in general, provided they cover data used for AI purposes and address AI-specific considerations.

The data governance framework also addresses data issues in third-party AI models, systems, or applications that the financial institution deploys, including where the financial institution provides prompts, internal documents, or other context to a third-party tool, or where the tool accesses the financial institution's data for its outputs (e.g. an LLM that accesses confidential or sensitive data for Retrieval-Augmented Generation (RAG)).

An effective data governance framework addresses the following AI considerations:

- alignment with the financial institution's risk appetite and strategy;
- clear accountability in different scenarios, including where the financial institution uses its own data, public data and/or data from third-parties;
- basic data literacy for all staff and additional, targeted training for staff working with data;
- resources needed for AI data processing, including computation and storage;
- procedures for the classification and labelling of data, including metadata;
- guidelines for processing unconventional data and data in different formats;
- data security including controls for (i) authorised access and data recovery and (ii) confidential and personal data (including privacy enhancing techniques);
- procedures for proper use of RAG, for example to confirm that data being retrieved and ingested are secure, representative and trusted; and
- an adaptable but consistent approach for assessing data quality and performance.

Effectively manage different stages of AI data use

Managing the different stages of AI data use is key to sound data governance. Effective management of these stages can vary by use case, but typically includes:

- an initial assessment of the availability, quality, quantity and suitability of data needed for the AI use case, which may in turn influence the AI design choice. This stage includes considering whether to use internal data, public data and/or data from third parties.

- a data collection stage that tracks and documents the authenticity and origin of data (data provenance). This stage can include due diligence on public and/or third-party data.[61]
- a data classification stage that documents the materiality, risk, sensitivity, intended and prohibited uses and other characteristics of data.
- a data preparation stage which may involve aggregating, annotating, cleaning, enriching, labelling, or updating data. This is an essential stage of the data management lifecycle and the most resource intensive.[62]
- an assessment of data quality after the data preparation stage and before deployment, which identifies gaps and limitations in the dataset as well as mitigating or compensating measures.
- post-deployment monitoring to identify and remediate problems that may be caused by data issues, such as data drift.

Documenting key steps throughout these stages is integral for tracking and understanding how data is enhanced, enriched, transformed and used as it flows through the financial institution (known as 'data lineage'), which can enhance data quality, facilitate auditability and aid the remediation of issues and risks, including root cause analysis.

Consider additional aspects for agentic AI

The way AI agents access, ingest, interpret, memorise, use and re-use data may affect their behaviour and outputs in ways that are difficult to detect. These data may be scattered across the financial institution's premises, the cloud and public sources - a 'federated' data environment. This can give rise to risks such as unauthorised access to or disclosure of sensitive data, which financial institutions manage by:

- strictly separating:
  - the agent's pre-defined goals (prompts), permissions (actions it is allowed to take) and rules (e.g. when to seek human approval); and
  - the data it can access to achieve these goals.
- applying appropriate access controls, classification and retention requirements to all data accessible to the agent, regardless of where the data are located or whether they are structured or unstructured ('context engineering').

---

61 For example, checking data generated by a GenAI model for accuracy and hallucinations before using that data to train another AI model or system.

62 This stage may include embedding 'instructions' in the metadata of data used by AI setting out the data's sensitivity, applicable legal requirements, permitted and prohibited uses etc. These instructions can act as guardrails on the actions the AI model, system or agent takes to fulfil its tasks (policy aware' data').

3.5. Explainability and transparency

Sound Practice 8 (Explainability and transparency): Financial institutions understand differences in the explainability of various types of AI. If appropriate and feasible, financial institutions adopt more explainable AI or consider compensating controls. Financial institutions also provide appropriate transparency tailored to different stakeholders.

In this report, explainability refers to the ability of an AI model or system to provide clear and interpretable outputs or decisions, specifically the extent to which humans can understand how an AI model or system generates outputs from inputs, including: (i) the factors, logic, or processes that contribute to outputs; (ii) the relative importance/weighting of input variables or features; and (iii) how methodological relationships vary across context or use cases. Explainability stems from characteristics in AI models or systems. It is not binary but a continuum.[63]

Transparency refers to the extent to which appropriate information about an AI model or system is made available to relevant stakeholders, including the financial institution's board and senior management, counterparties and customers interacting with the AI model or system and authorities. Transparency supports accountability, verification, assurance and auditability – especially for more material use cases.

Explainability and transparency are complementary but not synonymous. Even if appropriate information about an AI model or system is made available, it may still have inherent explainability limitations and neither its developers not its deployers may understand how it specifically translates inputs into outputs. Likewise, auditability/reproducibility and explainability are complementary and somewhat connected but distinct. Even if a financial institution maintains detailed lifecycle records and reproduces the outputs and actions taken by an AI model or system, it may not necessarily be able to explain how these outputs were derived.

Understand explainability

Financial institutions identify, understand and (where appropriate) communicate the degree of explainability of different AI models and systems for specific AI use cases. Financial institutions recognise that: (i) the importance of explainability may vary depending on the level of autonomy, materiality and risk of different AI models and systems; and (ii) explainability is not an end in itself but enables accountability, the assessment of conceptual soundness and compliance with legal and regulatory requirements.

Where justified, financial institutions consider trade-offs between explainability and performance. Limited explainability might be acceptable in some use cases. For example, in certain fraud detection use cases the superior predictive power of less explainable forms of AI may warrant their use. Conversely, AI that is heavily relied upon for credit decisioning, insurance underwriting, or other activities with potentially high impact on customers may warrant greater explainability.

---

[63] A related concept to 'explainability' is 'interpretability', which is the ease or difficulty of predicting what an AI model or system will do, i.e. the degree to which the cause of a decision can be understood.

There is a range of choices available to financial institutions to address explainability issues. These include building explainability into AI model or system development, using explainability methods and applying compensating controls where explainability is limited. The appropriate choice(s) will depend on the AI use case.

Build explainability into model development

During design and development financial institutions may create or select more explainable forms of AI if they do not perform significantly differently compared to more complex, less explainable forms. Financial institutions acknowledge that, all else equal, lower explainability increases the uncertainty about the AI model or system.

Apply explainability methods

Financial institutions apply explainability methods usually after the AI model or system generates its outputs ('post-hoc explainability').[64] These methods are generally applied when explainability challenges arise in model development. Financial institutions understand that: explainability methods vary in applicability, maturity and scope; have limitations that may introduce additional uncertainty; have prerequisite conditions to enable their functionality; and can involve trade-offs.[65] For example, analysis has identified limitations in the use of established explainability approaches when applied to AI.[66] Consequently, financial institutions:

- use explainability methods as part of a broader suite of AI risk management and mitigation tools, rather than as standalone solutions.
- avoid over-reliance on a single method. If appropriate, financial institutions combine two or more explainability methods (known as 'triangulation').
- recognise that explanations may be susceptible to assumptions, data characteristics or feature correlations and some explainability methods may themselves rely on additional models.[67]

Explainability methods can provide insights into the behaviour of AI models or systems at the global or local level. Both can be relevant and useful for understanding AI model or system behaviour, depending on the AI use case, its materiality and risk and the type of AI being used. For example, agentic AI systems that execute sequential decisions may warrant additional or different approaches to explainability that look not just at the agent's final output but intermediate decisions and steps.[68] In this manner, employing methods such as logs for AI agent activities can help humans track the agent's actions in real time or evaluate the actions after the fact (or both).

---

64 Examples of explainability methods include partial dependence plots and feature importance analysis.

65 See BIS-FSI (2025b).

66 See Cickovic and Serafino (2026) and Salih et al (2025).

67 See BOE (2025).

68 Financial institutions deploying multi-step agentic AI systems are developing explainability approaches that can trace and evaluate the full reasoning path, not the individual outputs.

- ‘Global explainability’ refers to how an AI model or system behaves overall. For example, in a ML credit scoring model, it refers to the key drivers of model output across all relevant borrowers. As another example, in an agentic system, global explainability would characterise typical execution patterns and common decision pathways.

- ‘Local explainability’ explains how an AI model or system delivered a given, single output. In the same ML credit scoring model, it refers to the key drivers of model output for an individual borrower. For the agentic system, local explainability would trace the specific sequence of reasoning steps,[69] tool invocations and intermediate decisions that led to the final, specific outcome.

Deploy compensating controls

Where explainability is constrained due to the complexity of AI models or systems, limited accessibility to information about the AI model or system, or third-party dependencies, financial institutions deploy compensating controls including:[70]

- guardrails, such as stricter limits on permissible use cases;
- benchmarking and/or the use of challenger models or systems;[71]
- sensitivity and stress testing;
- enhanced data governance;
- more extensive validation and testing; and
- increased human oversight, such as heightened scrutiny of outputs following deployment.

Compensating controls are particularly important in high-materiality and/or high-risk AI use cases, where they can help financial institutions accept limited explainability while mitigating risks.

If compensating controls cannot mitigate the risk stemming from the limited explainability of an AI model or system in line with the financial institution’s risk appetite and tolerance, the financial institution considers alternative solutions, such as deploying a more explainable AI or non-AI model or system, even if performance is inferior.

---

69 Some AI models or systems can be prompted to produce summaries of the rationale or reasoning behind their outputs in natural language (‘Chain of Thought prompting’), which may provide useful supplementary information. However, such explanations may not accurately or completely represent the factors that caused the model's behaviour and should therefore not be treated as an authoritative record how the model arrived at its output without additional validation.

70 See IAIS (2025) pp.27 and ECB Banking Supervision (2025).

71 A new, alternative, or retrained model or system that is tested against an existing, deployed model (known as the ‘champion’ model) to see if it can perform better.

Case study: Explainability for different AI models and systems

Traditional AI

A medium-sized bank engaging in retail lending is considering a traditional ML approach to increase earnings and reduce losses. Initial tests show that the ML model performs somewhat better, across several measures, than the non-AI model currently in use. However, the ML approach, which uses hundreds of features and involves complex interaction terms among them, presents considerable explainability challenges. These include a lack of understanding of how the ML translates inputs into outputs, which features are included in processing runs and how features are weighted. This lack of explainability creates some questions about the conceptual soundness of the ML approach. Furthermore, given that the ML is issued for retail lending, there are concerns about whether the ML approach might violate relevant consumer laws or regulations.

In response, the bank has chosen to include its consumer compliance experts into the process before the ML is deployed, to review both the input data and the output to monitor for potential discrimination or other bias against consumers. Those consumer experts identified some features that while not problematic themselves, have shown to be correlated with protected features (i.e. ones prohibited for use with consumers) - which are then dropped from the dataset. In addition, given the lack of ability to assess conceptual soundness in full, the bank places higher standards for performance and plans to conduct close and frequent monitoring of the ML approach over time. The bank also deploys some post hoc explainers to better understand how the ML processes inputs to produce outputs (while recognising the limitations of such explainers, for example if features are correlated with one another). Finally, the bank intends to use the ML approach in tandem with the previous non-AI model to benchmark the two sets of output and 'triangulate' around the most accurate outcomes.

GenAI

A large insurance company has decided to deploy an LLM-based AI system in its claims management unit to help claims adjustors with initial processing of customer claim submissions and other tasks. The LLM is a vendor-developed foundation model and the vendor itself has admitted that it does not fully understand how the LLM arrives at outputs for a particular input. The company has some concerns about the potential for hallucinations from the LLM and the inability to determine how they arise and how to minimise them.

In response, the insurance company decided to employ RAG based on its existing corpus of insurance information to help provide grounding information from which the LLM draws and thus help narrow the range of outputs. In addition, the company employs a reasoning feature with the LLM, to prompt it to demonstrate the steps by which it arrived at its output. However, the company is also mindful of recent research showing that some LLM reasoning may not be accurate, i.e. the LLM may be describing one set of steps to the operator/user but may actually be employing a different set of steps in its operation.

Given this level of uncertainty, the insurance company plans to deploy the LLM-based AI system in a controlled manner, with only partial deployment among some claims adjustors and only with qualified human oversight of the output before it is used. The company does not allow any LLM output to be shared directly with customers. Additional implementation of the LLM will only occur after further testing, including stability tests to confirm the LLM operates within a certain range. Furthermore, operators/users are given specific instructions for prompts, to help narrow the range of potential output and minimise hallucinations. Employees using the LLM are given proper training for its use, including clear indications of the LLM's limitations and parameters for its use.

Agentic AI

A large regional bank has decided to start deploying an AI agent for some operational tasks. It is pairing the agent with an LLM to provide information about steps to take. While the agent's supposed range of tasks involve a discrete, concise set of steps, the pairing with the LLM introduces a stochastic element to the agent's activities, given the probabilistic nature of the LLM. This means that there could be some

uncertainty about the steps to be taken by the agent should the LLM hallucinate or otherwise generate erroneous or problematic output - which could, in turn, cause the agent to duplicate tasks, conduct them in the wrong order, or attempt to operate outside its designated range of activity.

Controls deployed for use of the agent include prohibiting its use in any financial transactions until further testing is conducted, incorporating some intentional sensitivity tests by validators/reviewers to try to convince the agent to act beyond its established parameters. Finally, the bank conducts monitoring of the agent on a sampled basis, reviewing selected activities and tasks on a regular basis to confirm performance.

Consider transparency needs

Transparency is key for ensuring that both internal and external stakeholders are appropriately informed about the AI models or systems that affect them. For internal stakeholders, including those deploying an AI model or system developed by a third-party, transparency enables them to assess whether it continues to be fit-for-purpose and is performing as intended.[72] Increased transparency can also facilitate and inform financial institutions' engagement with authorities. For external stakeholders such as customers, transparency helps them understand the role AI plays in the products or services they use, and how AI may have influenced outcomes that are relevant to them. Overall, it is helpful to outline clearly how AI output is being used for key decisions within a financial institution.

Financial institutions make available appropriate information relating to their use of AI to internal and external stakeholders, which may include: the intended, permitted and prohibited uses of an AI model or system; its capability and its limitations; training data if available; and its development process. The optimal level of transparency may vary depending on the intended recipients of the information. Additionally, the degree of transparency may vary across different stages of model development and deployment and whether the model or system is developed internally or procured from a third-party AI provider.

Financial institutions tailor the information they provide to different stakeholders to support effective challenge and accountability, oversight and use of AI, while maintaining proportionality and avoiding undue complexity. Appropriate transparency involves providing information about how AI models or systems produce their outputs (subject to any explainability limitations referred to above) in ways that are understandable to the intended audience. Information provided to customers, authorities, auditors, risk managers, the board and senior management differ, reflecting differences in needs, expertise, responsibilities and decision making of these different stakeholders.

Provide transparency to customers and end-users[73]

Financial institutions consider the information needed for customers to understand the nature and limitations of financial products or services where AI plays a material role. Appropriate transparency does not necessarily entail financial institutions disclosing to end-users that they are using AI in all circumstances. However, it may include informing end-users: (i) that they are

---

[72] Consistent with Section 2.3, transparency can also assist with auditing and record-keeping,

[73] This section can also apply to investors.

interacting with AI (e.g. through chatbots); (ii) if AI might materially influence decisions that could affect them; (iii) if there are limitations associated with the AI model or system; and/or (iv) of their rights to appropriate explanations, contestability, or redress mechanisms (if applicable). Financial institutions may also consider offering 'opt-out' options or channels that allow customers to request a review of AI-generated outputs or human assistance.[74]

Case study: Transparency in AI-assisted loan decisioning

A credit union introduced an AI system to automate parts of its loan application process, including data entry and initial risk assessment, with final loan approval decisions made by human loan officers. Recognising that its members had a stake in understanding how their applications were being assessed, the credit union intentionally chose an AI technique with high explainability (intentionally *not* a "black box"), for example allowing identification of variables/features used and how they are weighted. Doing this allowed the credit union to inform loan applicants that AI was used in the initial stages of their application and provided them with the key factors that had influenced the preliminary assessment. Members were also made aware of their right to seek an explanation for a loan decision and to appeal if they believed the outcome was inaccurate and/or unfair. Furthermore, using an AI technique with high explainability helped the credit union confirm that it is meeting all relevant requirements in law and regulation related to this type of lending.

For internal stakeholders, loan officers had access to clear, explainable outputs from the AI system, including how inputs were processed into outputs, as well as risk identifiers and the reasoning behind them. This allowed credit union staff to exercise critical, informed judgement rather than simply deferring to the model's output and assessment. For example, when a member applied for a loan during a temporary layoff which is common practice in the cycle of a specific industry, the AI's assessment included contextual flags explaining the basis for its risk rating, allowing the loan officer to weigh this against the member's broader repayment history before making a final decision. The high explainability of the AI technique also allowed staff not involved in designing, building, or using the model to conduct an independent assessment of its conceptual soundness and provide an objective, critical assessment of the model performance and its intended use. In addition, the credit union continues to conduct ongoing monitoring of outcomes to confirm that the AI technique continues to remain reliable and fit for purpose.

3.6. Performance management

Sound Practice 9 (Performance management): Financial institutions evaluate the performance of AI use cases proportionately to their materiality and risk, including through performance assessments, testing and ongoing monitoring**.**

Assess dimensions of AI performance

Financial institutions evaluate AI performance across different dimensions, proportionately and over time (including via ongoing monitoring) and adapt their performance assessment to the objectives and anticipated outcomes of different AI use cases. They adjust the frequency, intensity, scope and types of performance assessment based on factors including:

[74] Depending on the jurisdiction and specific type of decision, fully automated decisions may not be permitted.

- the materiality and risk of the AI use case.[75] Material or high-risk AI use cases may justify higher performance requirements and a lower tolerance for errors.
- the AI model's or system's attributes, including complexity and scope of action. More complex models or systems may be more difficult to evaluate, while those with a broader scope of action may have greater downstream consequences if issues arise.
- the AI use case's prior performance. A model's or system's performance track record may signal where closer scrutiny is needed and helps financial institutions calibrate their assessment benchmarks.
- any recent changes to the AI model or system, or its data.[76]
- any significant changes to relevant real-world conditions.

Several types of performance assessments used for non-AI models or systems and other analytical approaches can help financial institutions assess AI models or systems.[77] Several key types are examined below (e.g. accuracy, benchmarking, range of output, robustness). Notably, financial institutions subject the performance of AI models or systems, in particular for high-materiality and/or high-risk use cases, to independent assessment by dedicated validation staff or others tasked with independent review.

Assessing the performance of traditional AI models or systems generally involves comparing a quantitative output with predetermined targets or thresholds (e.g. predicted versus actual quantitative values). It is therefore conceptually straightforward and easier to automate.

GenAI models or systems produce a range of potentially acceptable outputs but not necessarily a single correct output. Assessing GenAI performance is harder to automate and may involve more human judgment and qualitative metrics such as the coherence or relevance of an output.

Assessing the performance of agentic AI is a live area of research, which can be even more complex as it needs to consider not only whether the AI agent achieved its overall objective but also whether the actions it took to do so were appropriate.

Financial institutions assess dimensions of performance (individually and collectively) with the specific weighting of different dimensions and their corresponding performance measures determined by the AI use case. Dimensions of performance often include:

- *accuracy*: how close the output aligns with target or realised outcomes. Accuracy can be measured in different ways and along various horizons. Some AI models or systems may perform better in the short-term and others in the medium or long-term.
- *range of output* (also known as a 'confidence band' or 'distribution of outcomes'): whether output is centrally clustered or more widely dispersed, with a narrower range

---

75 MAS (2025b) pp.23.

76 See IAIS (2025) pp.25.

77 See BOE/PRA (2023) in particular Principles 3.3 and 4.4-4.5, Also see ECB (2025a), JFSA (2021), OSFI (2025b), and FRB et al (2026).

generally preferred. This dimension of performance can indicate how much uncertainty is associated with an output and whether a given point estimate is representative.

- *robustness*: how well the AI performs in new conditions or circumstances (also known as the ability to generalise to new data). Some forms of AI may experience natural degradation over time.

- *stability*: how reliable an AI model's or system's outputs are over time, including whether the same task performed or query asked at different times produces different outputs.[78]

- *sensitivity* or *stress testing*, during which extreme inputs or assumptions are fed into the AI model or system to determine the effects on outputs. This type of testing can help identify limitations and uncertainties of AI, including the conditions under which performance deteriorates or fails.

Financial institutions specify thresholds for all relevant dimensions of AI performance. These thresholds distinguish acceptable performance from those that warrant further investigation or indicate significant issues. Financial institutions monitor performance on an ongoing basis and assess cumulative trends, rather than rely only on results at a single point in time. Where possible, financial institutions define performance thresholds before the AI generate outputs (*ante hoc)* for both quantitative and qualitative measures. This is generally preferable to reviewing outputs after they are generated and retrospectively deciding what constitutes adequate performance (*post hoc)*. As noted above, this might be harder for certain types of AI, such as agentic AI. Financial institutions generally review performance thresholds periodically to confirm they are still appropriate.

Carry out developmental testing

Financial institutions carry out testing during the design and development stage ('developmental testing') to understand early on whether an AI model or system needs adjustments or additional calibration. Developmental testing typically covers the dimensions of performance noted above, where feasible. Financial institutions may also use this testing to decide whether a given AI use case (or its underlying model or system) is worth pursuing further.

Financial institutions' developmental testing generally considers how well an AI model or system performs, according to its intended use. This may include checking whether there is:

- *overfitting*, occurring when the AI model or system is narrowly focused on its training data, performing well for that training data but poorly on new data, contributing to a lack of robustness and inability to generalise;[79] and

- *unacceptable bias*, including statistical biases such as trading platforms favouring large-cap stocks or stocks in certain sectors. Biases can also lead to legal or regulatory

---

78 One helpful way to consider stability is the potential 'capability-reliability' gap, i.e. if an AI model or system is capable of executing operations but not consistently enough to be reliable.

79 There is evidence that AI models or systems can have a higher propensity for overfitting, compared to non-AI models and other quantitative approaches.

breaches or discrimination against certain groups or parties. Financial institutions test for unacceptable bias in various parts of an AI model or system, including its training data, its design choice, or how its output is used.

It may be challenging to identify and detect unacceptable bias, especially if a financial institution does not have access to the underlying dataset, or if the AI model or system has explainability limitations.

Case study: Developmental testing

A large internationally active bank began developing a ML model in its trading business with the expectation that it would perform better than the bank's current non-AI model. The bank developed an initial version of its ML model, conducting various tests to assess performance. Testing showed that the new ML model did not consistently outperform the existing non-AI model, including for stability. In addition, the training dataset was found to be not representative of the production data to be used with the ML model over time. Other aspects of the ML model did not fully align with the conditions in which it would be deployed. Given these substantive adverse outcomes, as well as the higher complexity of the ML model that made it more challenging to assess, the bank decided to postpone further deployment of the ML model and continue to use its existing non-AI model.

Conduct ongoing monitoring and testing

After confirming through developmental testing that the AI model or system can be responsibly deployed, financial institutions undertake ongoing monitoring and testing to: (i) confirm that the AI model or system performs well over time and relative to a range of realised outcomes; and (ii) support early identification of material deviations in results from the intended design and timely responses by the financial institution.

Financial institutions align the frequency, horizon, intensity, and type of ongoing monitoring and testing to the characteristics, materiality and risks of different AI use cases. Key steps in ongoing monitoring and testing may include:

- testing over time using new data, or data not used in training;
- repeating tests conducted prior to deployment;
- monitoring degradation in performance;
- confirming that the scope of activity remains within designated parameters;
- checking for data or model drift;
- periodically confirming that established performance metrics continue to be appropriate to the use case; and
- assigning staff to try to 'break' the AI model or system, or identify vulnerabilities, weaknesses and uncertainties ('red-teaming').

Financial institutions also use benchmarking where appropriate to evaluate AI performance by comparing an AI model's or system's output with output from other relevant models or systems, or other relevant information. Benchmarking is especially helpful when there are insufficient

realised outcomes against which to test the AI model's or system's output, or when attempting to triangulate accurate outputs. Benchmarking is most helpful when the alternative output has been produced by a model or system that takes a different perspective, such as using different data sources or methodologies.

As the number of AI use cases (in particular high-materiality and/or risk use cases) increases, financial institutions assess the resource implications, scalability and viability of different types of performance assessment and monitoring. Where appropriate, financial institutions explore ways to augment performance assessments potentially through automation.

Financial institutions recognise the challenges presented by AI models or systems that dynamically update – such as by drawing in new data, altering inputs, acting autonomously, changing feature relationships, or undergoing other modifications – and take steps to manage those challenges. In doing so, financial institutions maintain comprehensive, objective and appropriate testing, including developing new tests and conducting additional bias checks as needed. Financial institutions also conduct more frequent and intensive ongoing monitoring and alert relevant stakeholders about updates to AI models or systems. In certain cases, real-time continuous monitoring may be warranted, especially where AI acts dynamically or autonomously, has the potential to expand its scope of activity, is more complex, or is involved in a more material use case.

Financial institutions respond appropriately to performance assessment results based on the AI model or system, materiality, risk level and nature of findings. For example:

- poor results can indicate that the AI model or system needs updating, redeveloping, or retiring, or that contingency plans or alternative mechanisms should be triggered.
- results that indicate only mild concern might warrant further testing and closer monitoring.
- in certain cases, compensating controls, such as an overlay or other adjustment to outputs, might provide an appropriate response. Compensating controls can also include more intensive human oversight or limiting the use of the AI model or system to lower-risk areas until concerns abate.[80]
- in many cases compensating controls may be just temporary measures until more substantial steps can be taken to address underlying issues.

[80] One additional emerging type of control is purchasing insurance against adverse or unexpected AI outcomes. As with other types of insurance, it is important to define the terms of such insurance carefully (including limitations on coverage) and confirm that the insurer is sufficiently creditworthy. In this regard, the IAIS is currently exploring developments in the underwriting of AI risks as part of its Global Monitoring Exercise.

Case Study: Performance monitoring in a nonbank financial institution in an emerging market and developing economy (EMDE)

A digital fintech peer-to-peer lending company in an EMDE has implemented various machine learning models throughout their credit lending lifecycle, including underwriting, fraud detection in loan application, behavioural scoring and collections optimisation.

The company maintains a structured performance monitoring and governance framework to ensure that AI models continue to perform as intended after deployment. Monitoring dashboards are used for both underwriting and behavioural scoring models, providing reports over model outputs and portfolio performance. The company also conducts prediction distribution monitoring, population stability monitoring, feature shift monitoring based on population stability index, and default-rate monitoring to identify potential model degradation, data drift, or changes in customer behaviour. Validation staff conduct an independent review of the initial performance results, as well as monitor performance results over time.

In addition to continuous monitoring of obligors, they are periodically rescored using updated behavioural information to evaluate whether risk profiles have changed over time. Model versioning is implemented to support model development and facilitate comparison between existing and alternative models. All material model and credit policy changes require review and approval by the credit risk committee before implementation. This governance process helps ensure that the updated model remains aligned with the company's risk appetite, business objectives and credit portfolio performance expectations.

Consider additional aspects for GenAI and agentic AI

Financial institutions assess the compliance, explainability (if relevant), performance, reliability, resilience and safety of GenAI and agentic AI throughout their lifecycle.

Developmental testing of GenAI and agentic AI models or systems can give rise to additional challenges and considerations. For example, small linguistic changes to the input (prompt) of a LLM can significantly change the output, which increases unpredictability. Moreover, in certain instances, there may not be a 'ground truth' (i.e. verified, true data used for training and testing AI performance), meaning the assessment may not be as straightforward and financial institutions may include subject-matter experts as evaluators. Including a multi-disciplinary set of evaluators can help assess all dimensions of performance.

For agentic AI, monitoring involves continuous monitoring, and regular, routine assessment of specific actions or consequences (e.g. autonomous intermediate decisions and steps, interactions with the external environment) - and not just a review of the final output. Financial institutions monitor AI agents at runtime to detect drift, misuse, outages and threats (including attempts to manipulate prompts, context, tool outputs, memory or multi-step workflows). Monitoring covers key interim steps as well as final outcomes, so that financial institutions can see how an agent reached a result and whether it did so as intended, safely and within the bounds of its authorisations. Financial institutions use the results of continuous monitoring and evaluation as a key basis for deciding whether to grant agent more autonomy based on performance.

Testing assesses an AI agent's entire workflow, including how it accesses memory, follows orchestration logic, interacts with other systems or agents, retrieves information and uses tools. For agents with higher autonomy or posing higher risk, financial institutions apply adversarial testing, such as ethical red teaming.

Case Study: Performance testing for different AI models and systems

Traditional AI

A large internationally active bank has developed a new ML fraud detection and prevention model for its credit cards business. Initial tests demonstrate that this ML model outperforms the previous non-AI model used, including to reduce both false positive and false negatives. The bank continues further testing, including sensitivity tests, to determine the limits of the model and where it may not function as well. The bank also continues to collect information about realised outcomes to expand testing out of sample - especially to check whether the model may be overfit. Furthermore, the bank conducts ongoing testing for bias, including potential discrimination against certain consumers - especially since the ML model is quite complex and has some explainability challenges. The ongoing monitoring plan also includes checks for changes in fraud behaviour and activities to detect whether the established relationships in the ML model continue to apply.

GenAI

A medium-sized securities firm has deployed an LLM-based AI system to help with document retrieval and summarisation, including to evaluate prospectuses and draft outlines of public financial statements. The securities firm recognises that evaluating the blocks of text produced by the LLM can be challenging, especially since there is not a 'ground truth' against which to compare the output. The securities firm tasks certain employees to review the output of the LLM to determine the faithfulness to the underlying documents and check for hallucinations. Subject-matter experts are also tasked with evaluating the LLM's facility with more technical topics. Further testing includes checks for stability of output, such as running the same query multiple times and several hours/days apart to confirm that output is similar over time. Based on such testing, the securities firm determines that the LLM could continue to be used, but that a human has to review all output for accuracy before it is distributed within the firm. Also, staff using the LLM are given specific instructions to submit prompts and queries within certain parameters, to help narrow the range of potential output. Additional testing by subject-matter experts is conducted on a sampled basis.

Agentic AI

As a first step to experiment with AI agents, a large regional bank has started to deploy a few for simple operational tasks. The bank conducts testing on the full range of tasks the agent is permitted to execute, running repeated tests at different times to try to identify deviation in performance. In addition, some staff reviewing the AI agent make attempts to force it to take actions that are not permitted, for example, to see if it would try to access financial accounts. As the financial institution works with the agents, it collects information on performance, including from users. Use of the agents is limited to certain areas that do not involve financial accounts, areas requiring legal or regulatory compliance, or interactions with customers. Furthermore, one could direct the agent to follow regular checklists to confirm operational adequacy - if the agent does not follow the checklist or is unable to execute its steps, staff investigate further. Staff continue to monitor agent performance on a sampled basis.

3.7. Human oversight

> **Sound Practice 10 (Human oversight):** Financial institutions implement appropriate and effective human oversight relevant to the materiality, risk, autonomy, complexity and explainability of different AI use cases.

Effective human oversight has a tangible positive impact and supports responsible AI adoption (i.e. by improving decision-making, preventing harm, or providing redress). Effective oversight is

meaningful, i.e. it involves humans having sufficient ability, authority and incentive to intervene, as opposed to oversight that is nominal or driven by 'tick-the-box' compliance.

Design and develop appropriate and meaningful human oversight of AI

Financial institutions design and develop AI to enable effective and meaningful human oversight (as far as technically possible) which includes:

- enabling staff to assess the outputs of the AI model or system and understand its capabilities and limitations;
- preventing automation bias (i.e. overreliance)[81] by creating incentive alignment for thorough, thoughtful review, such as by incorporating performance metrics that reward quality of oversight decisions;
- creating feedback mechanisms for the AI model or system to learn and improve from oversight decisions, including tracking when humans override AI recommendations, analysing patterns in these interventions and using this information to refine both the AI model or system and the oversight processes; and
- assessing whether human overseers are providing effective oversight.

When obtaining an AI model or system from an open-source or open-weight repository or third-party AI provider, financial institutions consider the following as part of their due diligence:

- the extent to which the AI model or system has been designed to enable effective and meaningful human oversight by those deploying it; and
- (if applicable) the extent to which the third-party AI provider will provide human oversight. For example, in the case of a GenAI model, the extent of human oversight when the third-party AI provider deploys model updates and new versions.

Select appropriate forms of human oversight

Financial institutions select the most appropriate form(s) of human oversight taking into account the materiality, risk and other relevant factors, including technical feasibility, proportionality, resource effectiveness, as well as legal, regulatory and supervisory considerations. These forms are not mutually exclusive and may be used in conjunction, or separately at different stages of the AI lifecycle. Common forms of human oversight may include but are not limited to the following:

- *'Human-in-the-loop'*: human approval of all decisions made by AI, which might be appropriate in situations where accuracy is more important than speed of decision-making (e.g. approval of a health insurance claim).

[81] For example, an AI model or system may be designed to seek human feedback in specific scenarios or provide confidence scores for outputs.

- *'AI-in-the-loop'*: integrates AI into human oversight to augment performance monitoring rather than merely using humans to oversee AI. It uses AI as a supportive layer for decision-making and task automation while keeping humans in control (e.g. humans monitor and respond to AI-enabled automated alerts).[82] AI-in-the-loop may become warranted as financial institutions scale the number of AI use cases.

- *'Human-on-the-loop'*: human intervention periodically or only where necessary. For example, when the AI's outputs have a low confidence score or an override is necessary (e.g. AI chatbot autonomously handles routine customer inquiries, with human agents alerted to intervene only when sentiment analysis detects frustration or the request volume exceeds the AI's capability).

- *'Human-in-command'*: high-level human oversight, including deciding the extent of autonomy, setting guardrails and managing its overall impact. This form of human oversight is aimed at AI with high levels of autonomy, such as agentic AI.

- *'Kill switch'*: mechanisms enabling human intervention to halt or constrain AI operations, ranging from complete shutdown (which can be used in disabling algorithmic trading) to dynamic or graduated degradation where systems transition from autonomous to human operation.

- *'Contestability'*: mechanisms for human appeal and redress of AI outputs (e.g. allowing customers to appeal AI-enabled loan denials if they suspect unacceptable bias).

Set clear responsibility for human oversight throughout the AI lifecycle

The specific individuals responsible for human oversight and their related functions may change during the lifecycle of an AI use case. Financial institutions:

- allocate responsibility for monitoring an AI use case after deployment to staff who were not part of design and development to promote objectivity;

- document who the responsible staff are at different stages of the lifecycle, for example, by maintaining responsibility matrices; and

- tailor the training of staff to the lifecycle stage(s) they will be responsible for.

Consider additional aspects for GenAI and agentic AI

Some steps that financial institutions take for human oversight of GenAI include:[83]

- requiring a human to intervene when an LLM starts generating offensive, illegal, or inappropriate output.

---

[82] For example, agentic AI systems may automatically escalate to humans when accuracy metrics are beached or when requested by users, maintaining service while addressing performance issues.

[83] Various organisations are actively developing best practices for agentic AI. See for example NIST (2026).

- having humans periodically review and spot-check GenAI outputs to confirm consistency and stability over time.

- as a form of testing, having humans try to coerce an LLM to act outside its defined parameters ('jailbreak').

For agentic AI, financial institutions recognise that AI agents do not reason like humans and may interpret pre-defined goals in unexpected ways. The actions and capabilities of agents can also change over time, especially if they gain access to new tools or receive new prompts.[84]

a) Human oversight and deterministic controls

Financial institutions combine human oversight with deterministic (i.e. environmental or technical) controls to manage risks from agentic AI use cases proportionately. Deterministic controls are introduced at design and implemented as code in the control plane (the layer where decisions are made about what an agent can and cannot do). Combining human oversight with deterministic controls helps financial institutions manage the risks of agentic systems, which can be higher than for other forms of AI due to, for example, agents interacting with other agents, engaging in iterative reasoning loops, or repeatedly invoking tools in ways that can compound errors or trigger unintended actions.

Examples of combining human oversight and deterministic controls for agentic AI include:

- prohibiting agents from taking certain actions, such as those outside of the financial institution's risk appetite.

- where possible, training and deploying agents in secure environments.

    - In some use cases, this may include isolated, offline environments where the agent can only access pre-downloaded data and tools.

    - Where isolation is not possible, financial institutions define and, if appropriate, limit agents' abilities to interact with their external environment (APIs, data, ICT systems, networks, other agents etc.) to what is necessary. Financial institutions may also progressively increase an agent's ability to interact with the external environment as they gain confidence it can do so safely.

- setting clear, risk-based triggers for when an agent must seek human approval, confirmation or review. For example, before approving financial transactions above a certain value, or taking actions that may cause irreversible harm.

- breaking down an agent's pre-defined goals into discrete steps, with appropriate controls at each step that (if not met) can prevent the agent from moving to the next step.

---

[84] Some agentic systems limit the amount of information relevant to a specific task that an agent can access in a single session (context window) to manage consumption costs. Such limitation may lead to a situation where an agent may not 'remember' human prompts or other information relevant to safety from a previous session.

- defining an appropriate, risk-based frequency and operating model for human oversight, including triggers for transitioning between different forms of human oversight based on performance metrics or user requests.[85]

- using AI to continuously monitor AI agents, whilst evaluating the performance of monitoring tools to mitigate potential second order risks.

- monitoring and documenting anomalous behaviour that may indicate misuse or scope creep (e.g. an agent accessing data or customer records beyond what is necessary to achieve its pre-defined goals).[86]

- requiring agents to produce summaries describing their actions and associated reasoning. Where appropriate, financial institutions cross-reference and validate the accuracy and completeness of these summaries with other sources to mitigate the risk of deception and hallucination by agents.

- using 'red teaming' [87] and other forms of testing to assess whether AI agents can recognise problematic situations, avoid repeated errors, escalate to humans, stop safely, hand over to another process or return to a safe state without causing harm.

- implementing and testing risk-based 'kill-switch' mechanisms to pause, limit, override or remove an agent's access to systems, tools, databases or decision-making functions where appropriate. Testing may include how agents respond: when they cannot complete a task safely; when an external system they are connected to experiences failure or disruption; or when repeated, unsuccessful attempts to complete a step or task could make problems worse.

- ensuring operational resilience planning and testing for AI agents covers fallback processes, recovery expectations and escalation routes in a range of scenarios.

Higher-materiality and/or higher-risk AI agents use cases may warrant layered deterministic controls and more intensive human oversight. These measures are critical for constraining agent behaviour and reducing operational risk, but they do not, by themselves resolve questions about who is accountable for the agent's actions and outcomes. Financial institutions therefore typically complement such controls with explicit accountability arrangements. Internally, financial institutions assign and document accountable individuals for each AI agentic use case. Externally, financial institutions seek contractual clarity from third parties, including in relation to legal liability and apply compensating controls where appropriate.

---

85 In some cases, monitoring may need to be continuous or performed by AI. However, even when active monitoring is primarily undertaken by machines, financial institutions and individuals retain ultimate accountability.

86 This may include: the reasoning at each autonomous decision point; the APIs' data and other tools accessed by the agent; and the final outcome (including the agent's interpretation of success). This can improve staff's understanding of how an agent fulfilled its objectives (short of full explainability) and facilitate certain forms of human oversight (e.g. contestability, kill-switches, or overrides).

87 Red teaming is a structured testing effort to find flaws and vulnerabilities in an AI model or system, often in a controlled environment and in collaboration with developers of AI.

b) Orchestration, oversight of sub-agents and multi-agent interactions

In certain agentic AI use cases, AI agents may generate and orchestrate sub-agents to handle specific tasks and interact with other agents in the external environment. Financial institutions may also use agents from different third-party providers. These multi-agent interactions introduce additional layers of complexity to the human oversight of agentic AI systems. In these scenarios, financial institutions:

- monitor agent-to-agent interactions for risks such as cheating and collusion.[88]
- impose appropriate, consistent deterministic controls governing delegation to sub-agents.
- oversee agents and sub-agents at the orchestration layer where possible.
- develop consistent oversight frameworks for agents from different third-party providers.
- test how agents interact with other agents pre and post deployment, including through red-teaming.

Case Study: Agentic AI lifecycle management

A large life insurance company has made the choice to deploy AI agents in its consumer customer-facing operations, having conducted some analysis about potential cost and time savings, as well as lower error rates. Specifically, the company has begun to use agents in its consumer claims processing to automate certain manual tasks, such as receiving claims information, storing it, making initial assessments and responding to consumer customers. Since this is the company's first use of AI agents in the consumer space, they are particularly cautious. The company originally planned to use AI agents provided by a third party, but upon further consideration decided to build its own agents to achieve greater transparency about their operations, as well as higher levels of control over the agents.

As part of its initial steps, the company developed a set of standards and procedures for use of AI agents, including the following topics: identification, registration and authentication; levels of autonomy (minimal, constrained, full); permissioning and access; architectural controls vs procedural ones; execution plans; authorisation, decisions and prohibited activity; triggering conditions; agent interaction with the external environment (including customers, external systems and other agents); pre- and post-deployment validation (including proper testing); and scenario analysis, red-teaming and contingency plans.

As part of development, internal developers experimented with using single agents for individual tasks vs a multi-agent system orchestrated by a parent agent. For easier deployment of controls, the insurance company settled on a hybrid of the two, in which there is a parent agent, but use of sub-agents is quite limited and remains transparent. Initial testing in a protected environment also led to the company deploying additional controls for permissioning and access, given that during testing the agents could be coerced into trying to access databases and systems for which they did not have permission – in one case trying to delete certain data files.

Human oversight of the system involves several individuals, but one person remains ultimately responsible and accountable for the insurance company's overall (or organisation-wide) approach to the use of agents. For production, the company deployed these agents with constrained autonomy. It has put into place clear, strict controls for agent identification, so that each agent is individually registered and is tracked and monitored separately. Where possible, these controls are implemented

[88] This may include interactions among agents created using tools from different third-party providers.

at the control plane level to prevent access to sensitive assets, such as customer medical data, unless specifically allowed by a human overseeing the system of agents. The strict permissioning and access sought to prevent agent access to databases beyond approved ones. In particular, agents are given the minimum permissions necessary to accomplish their tasks. The appropriateness of these permissions is reviewed periodically and ahead of decisions to adjust agents' autonomy.

All agent actions during production are subject to automated, continuous monitoring with a log of activity and individual tasks. The log includes intermediate decisions and steps (not just final outcomes) that were escalated to human overseers and their outcome. Humans conducting oversight regularly spot-check key portions of agent logs to confirm there is traceability of actions – that the logs generated by the agents indeed match the actions taken by the agents. The company adopts a prudent approach to the oversight of its agents' activities, recognising that operational errors may occasionally occur and seeking to ensure that their impact is effectively contained.

Staff responsible for overseeing the agents conduct periodic tests to confirm that both individual agents – including sub-agents – and the overall agent system operate within their authorised permissions and assigned tasks. Furthermore, independent validation staff review the development, testing and implementation of the system of agents. Staff schedule periodic stops of agent activity, to review completed and on-going tasks. They also execute random pauses in activity for spot-checking, including to verify that sub-agent activity stops when the parent agent does. Until the insurance company spends more time reviewing and analysing agent activity (including any near-misses or unexpected problems), it does not plan to expand the materiality of agent tasks, nor the level of autonomy provided to its agents.

3.8. Cyber and ICT risk management

> **Sound Practice 11 (Cyber and ICT risk management)**: Financial institutions manage AI-related cyber and ICT risks, including, where appropriate, by incorporating AI cyber and ICT risk scenarios into tests and exercises, sharing relevant information and using AI tools in cyber and ICT risk management.

Adapt or enhance cyber security and ICT risk management to address AI risks

To effectively monitor, manage and mitigate cyber and ICT risks relating to AI (hereafter AI cyber and ICT risks), financial institutions adapt and enhance, as needed, existing practices on cyber and ICT risk management. There are extensive regulations, guidance, supervisory expectations, information bulletins, and practices on operational resilience, cyber and ICT risk management and third-party risk management by the FSB,[89] SSBs,[90] G7,[91] national authorities,[92] national cyber security agencies and other organisations active in the field of cyber and ICT risk management[93] that financial institutions can adapt. These measures can even be effective risk mitigants against the capabilities of advanced AI models, and include:

---

89 FSB (2020), FSB (2023a), FSB (2023b), and FSB (2025a).

90 For example, see BCBS (2021a); BCBS (2021b), BCBS (2025), CPMI-IOSCO (2016), and IAIS (2026).

91 For example, see G7 Cyber Expert Group (2020).

92 For cyber and ICT risk management in the use of AI at financial institutions, see for example BaFin (2026), APRA (2026), OSFI (2026), and BOE et al (2026).

93 See UK Department for Science, Innovation & Technology (2025a) and UK Department for Science, Innovation & Technology (2025b), Also see ANSSI (2025) and NIST (2025).

- cyber and ICT governance and cyber hygiene.
- reducing the potential attack surface by implementing strong network security to, among other objectives, limit attackers' ability for lateral movement in a compromised network. This may include:
  - documenting which systems are connected to the Internet and whether these connections are necessary for functionality; and
  - segmenting and micro-segmenting the most valuable ICT assets.
- implementing measures to monitor, prevent and remedy the use of 'shadow AI'.
- applying secure development practices to AI.
- authentication and 'identity and access management' (IAM) as well as phishing-resistant multi-factor authentication (MFA) to mitigate some of the risks of advanced AI models.
- adopting a multi-layered cyber defence strategy ('defence-in-depth') to AI so that, if one or more security layers were breached, the remaining layers are still effective in mitigating the risks. This is particularly important for advanced forms of AI, which can sometimes compromise certain layers, such as detection.
- applying secure-by-design principles to AI design, including performing threat modelling and incorporating security considerations during design, as well as implementing secure coding and code reviews during development.
- implementing security patches and updates promptly but securely, adopting risk-based prioritisation. Some advanced forms of AI are particularly adept at discovering vulnerabilities faster and at greater volume. They are also highly capable at chaining vulnerabilities to amplify their potential impact. This may accelerate the pace and volume of patching in future. Financial institutions assess if they can keep pace with compressed exploitation windows driven by AI-driven reconnaissance and exploitation, or if changes are necessary. Where patches are not yet available or cannot be applied immediately, financial institutions consider compensating controls such as virtual patching [94] to reduce exposure while permanent remediation is planned and implemented.
- enhancing monitoring and logging of anomalies and cyber incidents with controls on data provenance, cross-validation of datasets and model behaviour tracking.

[94] A security policy enforcement layer which does not fix a known vulnerability, but mitigates its exploitation, for example through monitoring of exploitation attempts and intercepts such attempts.

Understand and monitor AI cyber and ICT risks

Financial institutions use specialist sources of information to identify common, emerging and new AI cyber and ICT risks. These sources include:

- OWASP Machine Learning (ML) Security Top 10: an up-to-date list of the top 10 security issues of ML systems.[95] OWASP also publishes a top 10 list of security issues for agentic and LLM applications respectively.[96]
- MITRE ATLAS: a knowledge base of adversary tactics and techniques tailored to ML systems and covering the entire AI lifecycle.[97]
- NIST AI 100-2 E2025, Adversarial Machine Learning: a taxonomy and terminology of Attacks and Mitigation.[98]

In addition to these specialist sources, threat intelligence can help protect financial institutions and their customers from AI-related security threats. The importance of threat intelligence goes beyond vulnerability discovery. Where appropriate, financial institutions leverage attack surface intelligence to better understand not only potential vulnerabilities but also the systems and assets that may be vulnerable, so as to help prioritise addressing those weaknesses. Sources of threat intelligence may include:

- incidents and near-miss potential incidents at financial institutions, their peers and third parties;
- cyber scenarios, identified by the financial institutions, industry bodies and public authorities;
- specialist threat intelligence providers;
- vulnerability databases (see above); and
- open-source intelligence.

Use AI-powered tools to manage AI cyber and ICT risks

Financial institutions consider adopting AI-powered cyber and ICT risk management tools to adapt or enhance existing practices, including:

- AI-powered firewalls to help protect financial institutions against data exfiltration, harmful content and prompt injection attacks;

---

95 OWASP Machine Learning (ML) Security Top 10.

96 OWASP Top 10 for Agentic Applications for 2026; OWASP Top 10 for Large Language Model Applications .

97 https://atlas.mitre.org/.

98 NIST (2025).

- active liveness detection tools to detect deepfakes;[99]
- AI-powered behavioural analysis to detect anomalous behaviour, which can help detect distillation, pre-positioning, or prompt injection attacks;
- advanced AI models to identify and remediate vulnerabilities;
- threat modelling and vulnerability identification, using adversary tactics and techniques against AI-enabled systems based on threat intelligence;
- data loss prevention tools that use contextual understanding and behavioural monitoring to protect data against attacks such as privileged escalation;
- AI-augmented incident response, including automating incident response playbooks or speeding up forensic examinations and threat hunting to support humans in security operations centres; and
- using advanced AI models or agentic AI for autonomous cyber and ICT risk management, including automating aspects of vulnerability management (e.g. software updating and patching), security testing including source code reviews, penetration testing and adversarial simulation. Cyber security AI agents could even be used to combat agentic AI cyber attacks.[100]

Incorporate AI cyber and ICT risk scenarios in tests and exercises

Financial institutions incorporate AI cyber and ICT risks in their scenario testing, other forms of cyber and ICT testing (e.g. vulnerability scans) and exercises, especially for high-materiality and/or high-risk use cases.[101] Scenario testing allows financial institutions to assess and strengthen their ability to respond and recover from disruption, with a view to ensuring that their critical operations can remain within agreed tolerance for disruption in severe but plausible scenarios.

Case study: UK Cross-Market Operational Resilience Group

Some authorities and industry groups maintain scenario libraries to assist financial institutions in their scenario testing. Some have started including AI and cyber ICT scenarios in these libraries.

The Cross-Market Operational Resilience Group (CMORG), a public-private collaboration forum in the UK, maintains a Dynamic Scenario Library (DSL) which provides a structured, sector-wide catalogue of severe but plausible scenarios to support operational resilience planning and testing across the UK financial sector.[102]

The 2026 edition of the DSL introduced AI and cyber ICT scenarios. One scenario involved a threat actor using GenAI and agentic AI to bypass a financial institutions' internal controls and create staff accounts, which it then utilises to conduct criminal activities at scale (e.g. data theft, unauthorised transactions and fraud).

---

99 MAS (2025a).

100 There are currently fewer AI-powered tools for incident recovery, which may imply that this might be an area for future development.

101 IAIS (2026) sets out the important role for scenario analysis in maintaining operational resilience.

102 See CMORG website.

Exercises, such as tabletop, sector-wide and simulation exercises, are another valuable way to assess the ability of financial institutions and the financial sector as a whole (including third-party service providers) to coordinate and respond collectively to incidents.[103]

Financial institutions incorporate AI cyber and ICT risks in other types of testing. For example, 'red teaming' can test not just the performance of GenAI but also the vulnerability of AI models or systems against adversarial attacks such as prompt injection and model inversion and the effectiveness of associated controls.

Controlled environments are also used to test the capabilities and risks of emerging forms of AI.[104] For example, they could help monitor and understand the behaviour of AI agents before deployment into production. However, testing environments may not, by themselves, provide sufficient protection from cyber and ICT risks. Highly autonomous AI systems may devise ways to escape or evade these environments, which may in turn warrant additional controls and safeguards.

There might be potential to incorporate AI scenarios and tools in threat-led penetration testing (TLPT) in future. However, further work is needed to understand the ethical, legal and practical implications of doing so.

Collaborate and share information

Financial institutions establish or use mechanisms to securely share information on AI incidents, near-misses, deteriorating or unusual performance, risks, lessons learnt, threat intelligence and good practices. Such mechanisms include Information Sharing and Analysis Centres (ISACs).[105] Collaboration can also help financial institutions manage the increase in the speed and volume of vulnerability identification and remediation resulting from recent developments in AI (referred to above). Over time, proactive information-sharing can help to highlight additional sound and bad practices.

Consider additional aspects for agentic AI

Financial institutions adapt ICT controls to agents, including Identity and Access Management (IAM) and least privilege, which grants agents the minimum permissions needed to achieve their goals ('least agency').

Agentic IAM and least agency may include controls such as registration, continuous trust scoring, cryptographically verifiable credentials, lifecycle-managed permissions and scoped authority and authentication for agents interacting with the external environment or on behalf of customers. This includes 'dynamic IAM' for AI agents to address the limitations of IAM for human users.[106]

---

[103] See FSB (2023b) pp.40 and G7 Cyber Expert Group (2020).

[104] See, for example, AI Lab | FCA.

[105] See FS-ISAC | Advancing cybersecurity for the global financial system.

[106] Dynamic IAM (IAM) grants, modifies, or revokes user permissions in real-time based on context, such as user behaviour, device security posture and location. It uses Attribute-Based Access Control and AI to allow for continuous verification. It can minimise unauthorised access risks by adjusting access dynamically rather than manually or statically.

Financial institutions apply zero-trust principles to agents, such as explicit identity verification, least privilege access and action-level authorisation, to complement deterministic controls with human authorisation of key decisions at the point of action.

3.9. Third-party AI risk management

> **Sound Practice 12 (Third-party AI risk management):** Financial institutions appropriately manage risks from third-party AI dependencies with a focus on performance, transparency, data quality, supply chain and concentration risks and business continuity.

Leverage and adapt existing regulation and guidance on third-party risk management

Financial institutions leverage existing technology-neutral publications on third-party risk management issued by the FSB,[107] SSBs,[108] international bodies and authorities in several jurisdictions[109] as a foundation for managing third-party AI risks, adapting them as appropriate to consider AI-specific risks. In particular, financial institutions:

- conduct appropriate due diligence on prospective third-party AI providers.
- select an appropriate third-party AI provider considering business needs, risk considerations as well as legal and regulatory obligations.
- include contractual terms with third-party AI providers that enable: effective oversight and risk management, including monitoring rights;[110] access, audit and information rights; provisions on data access, quality and security, including responsibility for updating data and disclosure of processing jurisdictions; business continuity obligations; and termination rights.
- identify material AI components, functionality, services and tools embedded in third-party tools and services not explicitly marketed or sold as AI-enabled.[111] Where these create material AI dependencies on these tools and services, consider such dependencies in their concentration risk management and contingency planning.
- collaborate, including through industry groups to agree common assurance, information and contractual terms, as well as engage collectively with third-party AI providers to try and standardise them.[112]
- appropriately oversee the provision of third-party AI services. Financial institutions may (where appropriate) use independent auditors and pooled audits.

---

[107] See FSB (2023b).

[108] See, for example, BCBS (2025) and IAIS (2026).

[109] For example, see BOE/PRA (2021) and FRB et al (2023).

[110] This may include monitoring the incorporation or use of AI by third-party service providers of non-AI critical services within these services.

[111] This allows financial institutions to remain aware of material AI dependencies in these tools and services even where AI functionality is introduced after they are contracted for and deployed or embedded.

[112] See IAIS (2026).

Use AI transparency and assurance tools

Financial institutions obtain appropriate, risk-based assurance and information from third-party AI providers to understand, assess and manage relevant risks. This includes visibility into AI models and systems.

In addition to the materiality and risks of AI use cases, the level of transparency that financial institutions seek from third-party AI providers reflect their reliance on third-party AI, both individually and overall. Smaller financial institutions might be primarily 'deployers' of third-party AI. Larger financial institutions tend to rely on a combination of third-party and internally developed AI (although the latter often comprises third-party or open-source/open-weight components). Where a financial institution is a deployer of third-party AI, its ability to manage and mitigate AI risks may need to be reliant on or supported by assurance and information from third-party AI providers.

In addition to documentation, transparency and assurance tools, financial institutions' contractual arrangements with third-party AI providers address disclosure and notification of:

- arrangements for data usage, sharing and retention;
- material changes affecting AI behaviour;
- permitted and prohibited use;
- training approaches;
- service availability;
- underlying technology dependencies; and
- changes to third-party AI services (including non-AI services with embedded AI elements) that may alter risk profiles after deployment.

Additionally, where relevant, financial institutions' contractual arrangements clarify accountability for model performance, model drift, service degradation, version updates and service discontinuity, including liability for actions taken by highly autonomous AI agents.

Financial institutions enhance third-party AI transparency through various channels, including but not limited to legal and regulatory disclosures, AI model and system cards, as well as certifications and standards.

Financial institutions leverage disclosure obligations, where available. For example, in some jurisdictions, AI developers are required to publish or make available to organisations deploying their AI models, systems or applications information on: intended, prohibited and restricted uses; data; capabilities, characteristics and limitations (including on explainability); feasibility of human oversight; and cyber and ICT security. In some cases, third-party AI providers may also be subject to incident reporting obligations.

Financial institutions' contractual arrangements with third-party AI providers provide for the use of AI transparency and assurance tools. For example, AI model and system cards contain

information about AI models' or systems' data, functionality, use cases, potential biases, errors and limitations.[113]

AI certifications and standards provide assurance on the governance of third-party AI providers. A third-party audit is required to obtain certain AI certifications such as ISO/IEC42001, which provides a layer of independent validation.[114] However, while these certifications can provide partial or supporting evidence on the resilience of third-party AI providers, they may not be sufficient (by themselves) to satisfy financial institutions' responsibilities for due diligence and ongoing monitoring of third-party AI providers. Depending on the circumstances, financial institutions may consider whether additional due diligence or ongoing monitoring of third-party AI providers beyond these certifications is appropriate.

The AI transparency tools referred to above can help balance financial institutions' need for appropriate information from third-party AI providers, with the need of third-party AI providers to retain some commercially sensitive proprietary information.

A current limitation of AI transparency tools is that they are generally not tailored to the financial sector and may not cater to financial institution-specific risks and regulatory requirements. For example, model or system cards may provide information of how an AI model, system, or agent was built and its capabilities, but may not provide guidance on how financial institutions can integrate that model, system or agent safely into their environment (including constraints and guardrails).

Financial institutions could collaborate with authorities and third-party AI providers to develop targeted AI transparency and assurance tools (e.g. financial sector-specific model or system cards). In this regard, there are examples of these tools in some jurisdictions, such as a shared AI responsibility model.[115]

Consider compensating controls

If a financial institution cannot obtain sufficient assurance and information from third-party AI providers, it implements compensating controls. Although sub-optimal, these controls provide risk mitigation and may include: additional pre-deployment testing; limiting the initial use of the third-party AI to low materiality and risk use cases; and more intense human oversight (at least temporarily) such as enhanced monitoring, benchmarking, or stricter approval for certain actions. Contractual tools such as warranties and indemnities from third-party AI providers can also help compensate for limited transparency. Where there are no satisfactory compensating controls available to the financial institution that can bring relevant risks within agreed appetite, it may decide not to use the third-party AI provider's model or system.

---

[113] For example, see OECD Model Card Regulatory Check.

[114] See ISO/IEC 42001:2023 - AI management systems.

[115] For example, CMORG AI Shared Responsibility Model.

Monitor and manage concentration risks at the financial institution level

Financial institutions monitor and manage concentration risks at the individual financial institution (including group level). In particular, financial institutions monitor risks across the AI supply chain/ ecosystem and assess their potential impact on the services they use to the extent practicable and in line with proportionality.[116] This includes dependencies on:

- infrastructure service providers (e.g. cloud, compute);
- data providers;
- energy providers supporting AI infrastructure;
- foundation-model developers;
- specialised AI service providers; and
- hardware suppliers.

Incorporate business continuity, exit strategies and incident management

Financial institutions using third-party AI for high-materiality or high-risk use cases incorporate concentration risk considerations into their business continuity planning (which may include temporarily, risk-accepting diminished functionality if it falls within the financial institution's tolerance for disruption) and exit strategies. A financial institution may consider evaluating the volume and types of sub-contracted or sub-outsourced activities (i.e. where a third-party AI provider itself relies on external parties) and the degree to which the third-party AI provider relies on those subcontractors to further identify indirect concentrations risk.

As part of their operational resilience and third-party risk management framework, financial institutions assess whether critical services remain resilient, recoverable and subject to effective oversight when AI-enabled capabilities fail or become unavailable. Contingency planning considers:

- incidents caused by or involving AI models or system (whether accidental or malicious). For example, mass deletions of data, hallucinations, or cyber attacks committed by AI agents in the pursuit of pre-defined objectives;
- cloud-service disruptions;
- foundation-model degradation;
- vendor discontinuation; and
- infrastructure failures affecting AI operations

[116] For example, by asking a third-party AI provider how it has tested its ability to deal with severe shortages of essential hardware or energy.

Financial institutions also explore the use of joint scenario tests and sector exercises with third-party AI providers as a means to mitigate potential sector-wide risks.[117]

Financial institutions take steps to remain up-to-speed with changes and updates to third-party AI models and services, including cloud hosted AI services and manage relevant risks including drift, service continuity and declines in data quality, explainability, performance and transparency.

Case study: Financial institutions' management of risks from third-party AI dependencies

Some internationally active banks have uplifted their procurement and third-party risk management frameworks to address AI-specific risks. Common challenges these banks seek to address include information gaps (financial institutions often have limited visibility into third-party AI systems, such as training data, model details, or how their data is used by the vendor) and accountability gaps (financial institutions remain accountable for AI outcomes even when the AI was not built in-house).

These banks have developed internal frameworks for categorising common third-party AI deployment patterns, including: onboarding with customisation (e.g. fine-tuning); onboarding without customisation (including SaaS); and embedded AI within a wider product. They have recognised that 'open source' AI spans a spectrum, from fully open-source models to open-weights models and models with restricted-use licensing, with different risk and due diligence implications for each.

A key principle adopted is to subject third-party AI to the same lifecycle governance as in-house AI, with additional steps where vendor visibility is limited. The practices include:

- requesting standardised vendor disclosures (often via 'AI Cards') proportionate to risk;
- deciding how to respond when disclosures are incomplete, using mitigants such as indemnities, external attestations, or compensatory testing;
- conducting AI-specific due diligence during procurement and on an ongoing basis;
- monitoring for unapproved new AI features via vendor release notes;
- scheduling periodic reassessments and including contract notification clauses;
- updating contracts to cover AI-specific issues such as intellectual property, data retention, cybersecurity and change notification; and
- ensuring appropriate legal, technical and risk expertise is involved throughout.

[117] In some jurisdictions third-party service providers designated as critical service third-party providers by authorities are subject `to direct oversight by authorities. This can include engagement in joint incident management exercises with financial institutions.

Annex: List of Sound Practices for financial institutions' responsible AI adoption

Sound Practice 1 (Strategic direction and oversight): The board and senior management align AI adoption and governance with the financial institution's business model, risk appetite and strategy.

Sound Practice 2 (Governance and accountability): Financial institutions define clear roles and responsibilities and maintain an appropriate governance framework to enable responsible AI adoption.

Sound Practice 3 (Incorporation of AI risks into risk management framework and effective documentation of AI use): Financial institutions adopt risk management frameworks that effectively address AI risks and include processes for documentation of AI use, as well as for materiality and risk assessment.

Sound Practice 4 (Organisational adaptability): Financial institutions learn, adapt and adjust their oversight, governance, risk management practices and capabilities as AI evolves.

Sound Practice 5 (Materiality and risk assessment): Financial institutions implement an effective and systematic approach to assess the materiality and risk of AI use cases at the inception stage and thereafter.

Sound Practice 6 (Selection process): When selecting AI models or systems, financial institutions consider business objectives, operational and technical needs, as well as the materiality and risks of AI use cases.

Sound Practice 7 (Data governance): Financial institutions establish appropriate data governance to maintain data that is fit-for-purpose for training, testing and using AI (i.e. accurate, complete, consistent, reliable, secure).

Sound Practice 8 (Explainability and transparency): Financial institutions understand differences in the explainability of various types of AI. If appropriate and feasible, financial institutions adopt more explainable AI or consider compensating controls. Financial institutions also provide appropriate transparency tailored to different stakeholders.

Sound Practice 9 (Performance management): Financial institutions evaluate the performance of AI use cases proportionately to their materiality and risk, including through performance assessments, testing and ongoing monitoring**.**

Sound Practice 10 (Human oversight): Financial institutions implement appropriate and effective human oversight relevant to the materiality, risk, autonomy, complexity and explainability of different AI use cases.

Sound Practice 11 (Cyber and ICT risk management): Financial institutions manage AI-related cyber and ICT risks, including, where appropriate, by incorporating AI cyber and ICT risk scenarios into tests and exercises, sharing relevant information and using AI tools in cyber and ICT risk management.

Sound Practice 12 (Third-party AI risk management): Financial institutions appropriately manage risks from third-party AI dependencies with a focus on performance, transparency, data quality, supply chain and concentration risks and business continuity.

Glossary

This glossary provides **a non-exhaustive list of terms and definitions used in this 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. The definitions draw on the previous FSB reports on AI[118] and other relevant works,[119] and also on the extensive work that has previously been done or is underway by other groups in developing lexicons and glossaries related to financial institutions' AI adoption.

Agentic AI: A category of AI models (or systems) designed to function as autonomous agents capable of independently making decisions, learning from interactions, adapting to changing environments and optimising processes without direct human intervention. Unlike traditional AI models, agentic AI exhibits independent reasoning, goal-driven behaviour and the ability to interact dynamically with users, systems and real-world scenarios.

Artificial Intelligence (AI) model (or system): An AI is a machine-based model (or system) that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI models (or systems) vary in their levels of autonomy and adaptiveness after deployment.

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

Data drift: When data used to train, validate, test and run an AI model or system ceases to be appropriate. For example, because it no longer applies to current circumstances or when the relationships among features established by the AI methodology no longer hold.

Explainability: The ability of an AI model or system to provide clear and interpretable outputs or decisions, specifically the extent to which humans can understand how an AI model or system generates outputs from inputs. This includes: (i) the factors, logic, or processes that contribute to outputs; (ii) the relative importance of input variables or features; and (iii) how methodological relationships vary across context or use cases. Explainability stems from characteristics in AI models or systems. It is not binary but a continuum.

Foundation models: An AI model trained on broad data, generally using self-supervision at scale, that can be adapted to a wide range of downstream tasks.

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.

Human-in-the-loop: Human approval of all decisions made by AI, which might be appropriate in situations where accuracy is more important than speed of decision-making (e.g. approval of a health insurance claim).

---

[118] FSB (2024b) and FSB (2025b).

[119] For example, see FSB (2023a) and FSB (2023b).

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.

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.

Model drift: When the relationships between model inputs and outputs change. For example, because the assumed linkage between an independent (or input) variable and a dependent (or output) variable no longer holds.

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

Open-source model: An AI model made available under terms and in a manner that permit users to use, study, modify and share the model, with access to relevant information and components, such as relevant information about training data, source code used to train and run the model and model parameters, including weights.

Open-weight model: An AI model whose trained model weights are publicly available. Other components or information, such as training data, training code or documentation, may remain unavailable or restricted and terms governing use, modification or redistribution may vary. Availability of model weights alone does not make a model open source.

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

Retrieval-Augmented Generation (RAG): An AI technique that can improve LLM accuracy by retrieving data from a selected corpus of sources, such as internal company databases or live data feeds, to inform its outputs.

Shadow AI: AI tools adopted by employees of an organisation without authorisation or for unapproved uses, reducing the organisation's visibility of and ability to monitor and manage AI related risks.

Supply chain: The network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a financial institution. For the purposes of this report, the scope of supply chain is limited to the services under a third-party service relationship.

Traditional AI: A suite of computational techniques, such as longstanding machine learning methods, that pre-date recent advances, such as GenAI.

References

Australian Prudential Regulation Authority (APRA) (2026), *APRA Letter to Industry on Artificial Intelligence (AI)*, April

BIS Financial Stability Institute (BIS-FSI) (2025a), *Financial stability implications of artificial intelligence – Executive Summary*, June

BIS Financial Stability Institute (BIS-FSI) (2025b), Managing explanations: how regulators can address AI explainability, *FSI Occasional Paper*, No. 24, September

BIS (2025), *The use of artificial intelligence for policy purposes*, October

Bank of England (BOE)/ Prudential Regulation Authority (PRA) (2021), *SS2/21 Outsourcing and third party risk management*, March

BOE/PRA (2023), *SS1/23 – Model risk management principles for banks*, May

BOE (2025), *Model Risk Management AI and ML Roundtable - Current thinking and risks identified in artificial intelligence and machine learning (AI and ML) adoption*, October

BOE, Financial Conduct Authority (FCA) and HM Treasury (HMT) (2026), *BoE, FCA and HM Treasury joint statement on Frontier AI models and cyber resilience*, May

Basel Committee on Banking Supervision (BCBS) (2021a), *Principles for operational resilience*, March

BCBS (2021b), *Principles for the Sound Management of Operational Risk*, March

BCBS (2024), *Digitalisation of Finance*, May

BCBS (2025), *Principles for the sound management of third-party risk*, December

Board of Governors of the Federal Reserve System (FRB), Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration and Office of the Comptroller of the Currency (OCC) (2019), *Interagency Statement on the Use of Alternative Data in Credit Underwriting*, December

FRB, FDIC and OCC (2023), *Interagency Guidance on Third-Party Relationships*, SR 23-4, June

FRB, OCC and FDIC (2026), *Revised Guidance on Model Risk Management*, SR26-2, April

Bowman, M W (2024), *Artificial Intelligence in the Financial System*, Remarks at the 27th Annual Symposium on Building the Financial System of the 21st Century: An Agenda for Japan and the United States, November

Bowman, M W (2026), *Responsible Innovation and Financial Inclusion*, Remarks at "Next-Gen Financial Inclusion," the third annual Financial Inclusion Conference hosted by the Federal Reserve Board, July

Breeden, S (2024), *Engaging with the machine: AI and financial stability*, Speech given at the HKMA-BIS Joint Conference on Opportunities and Challenges of Emerging Technologies in the Financial Ecosystem, October

Breeden, S (2026), *Agents of change*, Speech given at ECB Sintra Forum, June

Cickovic, I and A Serafino (2026): *Explainability in machine learning: do popular methods deliver on their promises?*, Bank Underground, June

Committee on Payments and Market Infrastructures (CPMI) and Board of the International Organization of Securities Commissions (IOSCO) (2016), *Guidance on cyber resilience for financial market infrastructures*, June

European Central Bank (ECB) (2024), The rise of artificial intelligence: benefits and risks for financial stability, *Financial Stability Review*, May

ECB Banking Supervision (2025), *ECB guide to internal models*, July

Federal Financial Supervisory Authority (BaFin) (2026), *Guidance on ICT Risks in the Use of AI at Financial Entities*, January

Financial Markets Standards Board (FMSB) (2026), AI in Trading: A practitioners' view of the current landscape, *Spotlight Review*, February

Financial Services Agency (JFSA) (2021), *Principles for Model Risk Management*, November

FSB (2013), *Principles for an Effective Risk Appetite Framework*, November

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

FSB (2020), *Effective Practices for Cyber Incident Response and Recovery*, October

FSB (2023a), *Cyber Lexicon: Updated in 2023*, April

FSB (2023b), *Final Report on Enhancing Third-party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities*, December

FSB (2024a), *Guidance on Arrangements to Support Operational Continuity in Resolution - Revised version*, March

FSB (2024b), *The Financial Stability Implications of Artificial Intelligence*, November

FSB (2025a), *Format for Incident Reporting Exchange (FIRE), Final report*, April

FSB (2025b), *Monitoring AI Adoption and Related Vulnerabilities in the Financial Sector*, October

FSB (2026), *Sound Practices for financial institutions' responsible AI adoption: Overview of consultation responses*, October

G7 Cyber Expert Group (2020), *G-7 Fundamental Elements of Cyber Exercise Programmes*, December

G7 Cyber Expert Group (2025), *G7 Cyber Expert Group statement on Artificial Intelligence and Cybersecurity*, September

Hlophe, N and L Mabetha (2025), *Artificial Intelligence in the South African Financial Sector*, Financial Sector Conduct Authority and South African Reserve Bank/Prudential Authority, November

Hong Kong Monetary Authority (HKMA) (2024), *Research Paper on Generative Artificial Intelligence in the Financial Services Sector,* September

HKMA (2025), *Responsible Innovation with GenA.I. in the Banking Industry – Practical Insights from the Generative Artificial Intelligence Sandbox,* October

HKMA (2026), *Regulators launch GenA.I. Sandbox++ to foster A.I. innovation across financial services*, Press Release, May.

International Association of Insurance Supervisors (IAIS) (2025), *Application Paper on the supervision of artificial intelligence*, July

IAIS (2026), *Application Paper on operational resilience objectives and toolkit*, February

International Monetary Fund (IMF) (2024), Advances in Artificial Intelligence: Implications for Capital Market Activities, *Global Financial Stability Report*, Chapter 3, October

IOSCO (2025), *Artificial Intelligence in Capital Markets: Use Cases, Risks and Challenges – Consultation Report*, March

IOSCO (2026), *Supervisory Toolkit for AI Use in Capital Markets – Final Report*, May

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2023) *ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system,* Edition 1

Lim, X-L, P Singh and R Stobo (2025) Regulatory Considerations Regarding Accelerated Use of AI in Securities Markets, *IMF Technical Notes & Manuals*, Volume 2025, Issue 016

Machado, P (2026), *Technology is neutral, governance is not: AI adoption in the banking sector*, Speech at KPMG RiskTech Conference, February

Monetary Authority of Singapore (MAS) (2024), *Artificial Intelligence (AI) Model Risk Management*, December

MAS (2025a), Cyber Risks Associated with Deepfakes, *Information Paper*, September

MAS (2025b), *Consultation paper on Guidelines for Artificial Intelligence (AI) Risk Management*, November

National Cyber Security Agency for France (ANSSI) (2025), *Building trust in AI through a cyber risk-based approach*, February

National Institute of Standards and Technology (NIST) (2023), *AI Risk Management Framework (AI RMF 1.0)*, January

NIST (2025), *Adversarial Machine Learning - A Taxonomy and Terminology of Attacks and Mitigations*, March

NIST (2026), *Announcing the "AI Agent Standards Initiative" for Interoperable and Secure Innovation*, News, February

Office of the Superintendent of Financial Institutions (OSFI) (2023), *Financial Industry Forum on Artificial Intelligence (FIFAI), A Canadian Perspective on Responsible AI*, April

OSFI (2025a), *FIFAI II: A Collaborative Approach to AI Threats, Opportunities, and Best Practices, Workshop 1 - Security and Cybersecurity*, July

OSFI (2025b), *Guideline E-23 – Model Risk Management (2027)*, September

OSFI (2026), *Frontier Artificial Intelligence: Implications for Technology, Cyber Security, and Operational Resilience*, Technology Risk Bulletin, April

Organisation for Economic Co-operation and Development (OECD) (2024), *Regulatory Approaches to Artificial Intelligence in Finance*, September

OECD (2026), *Supervision of artificial intelligence in finance*, January

Salih, A M, Z Raisi-Estrabragh, I B Galazzo, P Radeva, S E Petersen, K Lekadir and G Menegaz (2025), *A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME*, Advanced Intelligent System, Vol. 7 Issue 1, January

Swiss Financial Market Supervisory Authority (FINMA) (2024), *Governance and risk management when using artificial intelligence*, FINMA Guidance 08/2024, December

The MindForge Consortium (2026), *AI Risk Management: Operationalisation Handbook*, January

UK Department for Science, Innovation & Technology (2025a), *Code of Practice for the Cyber Security of AI*, Guidance, January

UK Department for Science, Innovation & Technology (2025b), *Implementation Guide for the AI Cyber Security Code of Practice*, January