

Public Disclosure Authorized  
**FINANCE**  
Public Disclosure Authorized

**Prosperity Insight Series**

Public Disclosure Authorized

# **ARTIFICIAL INTELLIGENCE FOR FINANCIAL SECTOR SUPERVISION**

Public Disclosure Authorized

## **An Emerging Market and Developing Economies Perspective**

**Report submitted to the G20 Finance Ministers and  
Central Bank Governors**

Gian Boeddu, Erik Feyen, Serafin Martínez Jaramillo, Sergio Mesquita, Yasemin Palta,  
Arpita Sarkar, Srishti Sinha, and Alexandra Gutiérrez Traverso

# ARTIFICIAL INTELLIGENCE FOR FINANCIAL SECTOR SUPERVISION

---

## An Emerging Market and Developing Economies Perspective

**Report submitted to the G20 Finance Ministers and  
Central Bank Governors**

Gian Boeddu, Erik Feyen, Serafin Martínez Jaramillo, Sergio Mesquita, Yasemin Palta,  
Arpita Sarkar, Srishti Sinha, and Alexandra Gutiérrez Traverso



A verified reproducibility package for this publication is  
available at <http://reproducibility.worldbank.org>, click [here](#) for  
direct access.

© 2025 The World Bank  
1818 H Street NW, Washington DC 20433  
Telephone: 202-473-1000; Internet: [www.worldbank.org](http://www.worldbank.org)

Some rights reserved

This work is a product of The World Bank. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean the World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

#### **Rights and Permissions**

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

**Attribution**—Please cite the work as follows: “World Bank. 2025. Artificial Intelligence for Financial Sector Supervision: An Emerging Market and Developing Economies Perspective. © World Bank.”

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e mail: [pubrights@worldbank.org](mailto:pubrights@worldbank.org).



# TABLE OF CONTENTS

<b>Executive Summary</b>	<b>1</b>
<b>1. Introduction</b>	<b>5</b>
<b>2. AI Adoption by the Financial Sector</b>	<b>7</b>
2.1 Current state of AI adoption	7
2.2 Outlook	2
<b>3. AI Adoption by Financial Sector Authorities</b>	<b>14</b>
3.1 Current state of AI adoption and outlook	14
3.2 Current and future use of AI for supervision	19
3.3 Challenges to AI adoption for supervision	22
3.3.1 Skills gaps and workforce readiness	23
3.3.2 Data quality and AI model training and validation	24
3.3.3 Digitization and integrating AI into existing systems and processes	25
3.3.4 Use of cloud infrastructure	26
3.3.5 Legal and regulatory challenges related to data privacy and security	27
3.4 Risks associated with AI adoption for supervision	29
3.4.1 Data privacy and security	30
3.4.2 Cybersecurity	30
3.4.3 AI model challenges	31
3.4.4 Operational risks	32
3.4.5 Vendor-related risks	33
3.5 AI governance and risk management	34

<b>4. AI-Related Consumer Risks and Supervision</b>	<b>37</b>
4.1 Supervisory perceptions of consumer risks	38
4.2 Supervisory responses to consumer risks	41
<b>5. Coordination and Collaboration</b>	<b>44</b>
5.1 Between domestic authorities	45
5.2 Public-private engagement	45
5.3 Across borders	46
<b>6. Looking Ahead</b>	<b>48</b>
<b>References</b>	<b>50</b>
<b>ANNEX: Survey and Interview Participants</b>	<b>54</b>

# GLOSSARY

AE	Advanced Economies
AI	Artificial Intelligence
AML/CFT	Anti-money laundering and countering financing of terrorism
ASIC	Australian Securities and Insurance Commission
BCB	Central Bank of Brazil
BIS	Bank for International Settlements
CCAF	Cambridge Center for Alternative Finance
ECB	European Central Bank
EMDE	Emerging Market and Developing Economies
EU	European Union
FCP	Financial Consumer Protection
FSB	Financial Stability Board
FSCA	South African Financial Sector Conduct Authority
G20	The Group of Twenty
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
IAIS	International Association of Insurance Supervisors
ICT	Information and Communication Technology
IT	Information Technology
KYC	Know Your Customer
LLM	Large Language Models
MC	Market Conduct
ML	Machine Learning
NLP	Natural Language Processing
OECD	Organisation for Economic Co-operation and Development
PA	Prudential Authority within the South African Reserve Bank
PoC	Proof of Concept
SupTech	Supervisory technology

# Acknowledgements

This report was prepared by a team led by Gian Boeddu and Erik Feyen and included Serafin Martinez Jaramillo, Sergio Mesquita, Yasemin Palta, Arpita Sarkar, Srishti Sinha, and Alexandra Gutiérrez Traverso. Harish Natarajan and Niraj Verma provided overall guidance. We would like to thank Alwaleed Alatabani, Hillary Allen, Sharmista Appaya, Ezio Caruso, Matei Dohotaru, Juan Carlos Izaguirre, Stela Mocan, Ilias Skamnelos, Kimmo Soramäki, and Bryan Zheng Zhang for discussions and suggestions. We are grateful to the participating authorities for their valuable insights and inputs (see Annex).





## EXECUTIVE SUMMARY

**Artificial intelligence<sup>1</sup> (AI) has the potential to transform the provision of both financial services and supervisory practices in emerging market and developing economies (EMDEs).** Increasingly powerful AI tools can transform the financial sector, ushering in new possibilities and challenges and prompting financial sector authorities to adapt. However, while AI's potential benefits and risks are widely recognized, knowledge gaps remain regarding the adoption of AI in EMDEs, including for financial sector supervision. At the request of the South African G20 Presidency,<sup>2</sup> this report provides an overview of the state of AI adoption for financial supervision in EMDEs. The report analyzes the results of a survey of 27 financial sector authorities in EMDEs worldwide, including 17 in Africa, as well as interviews with several of these authorities. The analysis was further enriched by discussions with selected financial authorities in advanced economies (AEs).

- 
1. Following OECD (2024), this report refers to AI in a broad sense: “machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”. Concretely, AI ranges from more traditional machine learning (ML) algorithms and applications which are typically used for narrower tasks such as classification through to more recent Generative AI (GenAI) innovations such as large language models (LLMs). Generative AI refers to systems that create new content, such as text, images, or code, based on patterns in the data they were trained on.
  2. The South African G20 Presidency requested that the Financial Stability Board and the Bank for International Settlements prepare reports on monitoring AI adoption and related financial sector vulnerabilities (FSB, 2025) and the use of AI for central bank policy purposes (BIS, 2025), respectively.

**AI could reshape business models, market structures, and consumer behavior in the financial sector.** It offers opportunities to improve efficiency, broaden inclusion, and strengthen oversight, but also introduces new challenges, including concerns related to data issues, reliance on third-party service providers (e.g., cloud services and AI models), model transparency and accuracy, and cybersecurity—and may bring transitional disruptions.

**AI use in the financial sector—which has important implications for financial supervision—is nascent in EMDEs and varies across countries and stakeholders.** Financial institutions are increasingly turning to AI for a host of tasks, from customer service to fraud prevention and regulatory compliance, with implications for financial supervision, although adoption remains limited in EMDEs. AI adoption in EMDEs lags their peers and the industry—led by fintechs—is typically ahead of financial sector authorities. Most authorities, specifically in non-African EMDEs, expect AI to deliver a net positive impact in the financial sector, in particular those reporting higher AI adoption by supervised institutions.

**Financial sector authorities in EMDEs are beginning to harness AI-powered tools for their supervision activities, but most are still at an early stage.** The adoption of AI is a board-level priority for most authorities, including for supervisory tasks, which are becoming more demanding and data intensive. Some authorities in EMDEs are gradually moving from early explorations of machine learning (ML) to more advanced applications, spurred by the recent surge in generative AI (GenAI). In addition, as part of more routine applications of AI, many authorities are using off-the-shelf GenAI tools for drafting and summarizing documents. Some are working to deploy AI agents, chatbots, and other GenAI-based tools for more sophisticated tasks such as internal knowledge management, complaints analysis, and

risk and compliance assessments of supervisory documents.

**Recent advances in AI have the potential to make supervisory technology (SupTech) tools more efficient and enable their application to more complex tasks, augmenting or automating work previously only undertaken by humans.** However, most financial authorities in EMDEs are still in the early stages of using AI—and none in Africa—for core supervisory tasks such as data collection, on- and off-site supervision, asset quality review, and anomaly detection, with some currently conducting tests and pilot programs. Yet, many authorities—including in Africa—are developing use cases and expect to launch new AI-driven SupTech initiatives within the next 12 months. One authority implemented a tool that examines the credit portfolio of a supervised institution and identifies exposures with inadequately recognized expected credit losses. In fraud and illicit finance analysis, another regulator uses AI to identify “mule accounts” (used to transfer illicit funds on behalf of others) and evaluate the efficiency of regulated institutions in tackling these challenges.

**Many EMDE authorities, including in Africa, are establishing formal AI policies and strategies to promote efficiency and innovation while addressing risks.** Some authorities already have a formal governance framework in place, with those in Africa lagging. However, many of the authorities that currently lack a formal framework expect adoption within the next 12 months, particularly in Africa. Authorities are taking varied approaches to testing and developing AI use cases. All interviewed EMDE authorities are putting governance frameworks in place to oversee organizational AI use, including centralized oversight mechanisms such as internal committees. Many are mapping supervisory processes to identify areas where AI can add the most value. Some are more proactive, encouraging departments to experiment broadly, while others are more cautious, limiting AI experimentation to

certain types of projects or supervisory business lines.

**Despite this progress, EMDE authorities face several key challenges to adopting AI, amplified by resources and infrastructure constraints.**

Unlocking and managing large amounts of sensitive data – currently often fragmented or in not readily useable or accessible form – while also complying with privacy, cybersecurity, and data localization rules poses challenges for authorities seeking to integrate AI into their supervisory processes. Authorities have diverse approaches to leveraging cloud services for AI with issues such as vendor dependency, data security, and data sovereignty emerging as common challenges. Some authorities have updated their legal and regulatory frameworks to permit cloud usage, while others have chosen to maintain data storage and processes on premises to minimize data protection and operational risks. Integrating new AI systems into existing and often outdated infrastructure can be cumbersome. As a result, several authorities are strengthening their foundational IT and data infrastructures. Many authorities, especially in Africa, cite skill gaps and struggles to attract and retain talent as fundamental challenges, and are investing in enhancing workforce readiness for AI. Several authorities take a strategic approach to embedding the necessary skill sets within supervisory teams, combining both domain knowledge and relevant technological expertise.

**Risks associated with AI adoption by EMDE authorities are diverse, with maintaining public trust being a core objective.** Cybersecurity threats and data breaches are seen as key risks, prompting authorities to safeguard systems and develop strong governance frameworks. Most authorities rely on the outsourcing of critical IT and AI infrastructure, typically with a small set of global vendors, amplifying vendor-related and concentration risks. Large-scale use of AI may also amplify operational risks. Inappropriate use of AI,

such as overreliance on AI tools for supervision in substitution of supervisory judgment, may result in compromised supervisory effectiveness and reputational damage. Several authorities stress that AI should not replace supervisory judgment and discretion, and that supervisors should retain final authority over AI-assisted supervisory decisions and be able to explain their rationale. Well-documented concerns about AI—such as those regarding model transparency, explainability, accuracy, accountability, and biases—are recognized by EMDE authorities, but these risks are not yet sufficiently addressed, as AI adoption is still in its early stages.

**In authorities that are more advanced in their use of AI, there is greater attention to such risks, but it is too early to tell whether it is sufficient.**

Some authorities restrict AI use to specific use cases and maintain vigilant human supervision. Examples include fraud detection in payment systems oversight, credit risk analysis, and sentiment analysis on social media and complaints monitoring and classification. To mitigate these risks, some authorities are enhancing capacity and infrastructures and developing contingency arrangements.

**EMDE authorities lack the capacity to monitor AI developments in the financial sector and assess impacts.** Although most authorities have limited ability to monitor AI developments and evaluate their impacts on financial institutions and consumers, many are engaging with the industry to collect and exchange information.

**EMDE authorities will likely need to increase their focus on AI-related consumer risks as financial institutions continue to adopt AI.** They display varying levels of readiness to understand and address these risks. Authorities are mostly preoccupied with AI-related fraud and scams by third parties. Risks to consumers stemming from cyber and data security and privacy are also of clear concern. However, authorities' risk perceptions

vary significantly regarding other AI-related risks to consumers resulting from adopting by financial institutions, such as model bias and discrimination, lack of explainability, lack of transparency, and manipulation of decision-making. These perceptions may change as AI becomes more deeply embedded in consumer-facing services in EMDEs and thus supervisory awareness of relevant consumer issues increases. Authorities are currently not creating new or revised AI-specific regulatory requirements when it comes to AI-related consumer risks. Rather, authorities can use a robust general consumer risk-assessment methodology supported by a comprehensive general financial consumer protection (FCP) regulatory framework.

**Most EMDE authorities agree on the importance of strong coordination and collaboration for the responsible adoption and effective oversight of AI in the financial sector.** Almost all financial authorities indicate a need for collaboration with other domestic regulators—such as those overseeing data protection and cybersecurity—to share information, address potential regulatory gaps and overlaps, and ensure consistent understanding of AI-related expectations. Equally important is engagement with the private sector: many authorities are exchanging information and encouraging responsible innovation through surveys, roundtables, and regulatory sandboxes.

Authorities in more technologically advanced EMDEs have started issuing guidance on AI use in the financial sector. Cross-border exchange of information and best practices are also widely regarded as essential, particularly for authorities that supervise institutions with international operations. Most EMDE authorities signal a need for international guidance to address regulatory arbitrage and tackle the cross-border nature of AI technology and service providers.

**While experiences differ across EMDE countries, several preliminary considerations for EMDE authorities emerge from this report.** These considerations, discussed in more detail in the report, relate to: taking a strategic approach to AI adoption; focusing on foundational IT and data issues; addressing skills and knowledge gaps; strengthening monitoring of AI developments in the industry, including risks; and fostering coordination and collaboration across domestic and international stakeholders. In particular, supervisors should retain final authority over AI-assisted supervisory decisions and be able to explain their rationale. Moreover, financial institutions must gain a thorough understanding of their AI applications and be accountable for model outputs and decisions. Domestic and international cooperation is essential to share information and best practices and address blind spots, inconsistencies and risks.

# 1c

## INTRODUCTION<sup>3</sup>

**Recent, rapid technological advances have produced more powerful AI tools with the potential to strengthen financial supervision in emerging market and developing economies (EMDEs).** AI-supported Supervisory technology (SupTech) has the potential to make significant contributions and can be especially helpful to financial sector authorities in EMDEs, which typically face more acute resource constraints compared to their counterparts in advanced economies (AEs). However, a knowledge gap exists regarding the current state of AI adoption by EMDE authorities and the related opportunities and risks. In this context, the 2025 South African G20 Presidency requested that the World Bank take stock of AI

developments in EMDE financial sector authorities, with an emphasis on financial supervision and with a strong representation of African EMDEs.

**The primary focus of this report is to contribute to a better understanding of the state of AI adoption in supervision by EMDE financial sector authorities and the associated practical issues, challenges, and risks they face.** This report focuses on EMDEs to complement existing work on global AI adoption and governance by central banks (e.g., Consultative Group on Risk Management 2025), AI for risk-based supervision in the financial sector (e.g., Dohotaru et al. 2025), SupTech adoption by financial sector authorities (e.g., Cambridge



Suptech Lab 2024), regulating AI in the financial sector (e.g., Crisanto et al. 2024), and the financial stability implications of AI (e.g., FSB 2024). The focus on African authorities also builds on other World Bank work on digital infrastructure in Africa (e.g., World Bank 2024). The audience for the report includes EMDE financial sector authorities and their government partners, as well as the range of other domestic and international stakeholders that participate in supporting improvements in financial sector supervision in EMDEs, including through leveraging SupTech.

**The report is not intended to be a ‘how to’ guide on AI implementation in EMDE authorities but rather aims to assist EMDE authorities and other stakeholders in having a better awareness of common challenges and how they are being addressed in an EMDE context.** Based on these findings, the report also offers preliminary, forward-looking considerations for EMDE authorities in addressing such challenges.

**As a secondary focus, the report examines how financial sector authorities are beginning to identify and monitor AI-related risks specific to financial consumer protection (FCP) and market conduct (MC).** Since this area has received

limited attention in EMDEs to date, the report aims to complement broader research on AI-related consumer risks as well as analysis from other perspectives, such as financial stability risks (e.g., FSB 2024). To provide further context for both of its focus areas, the report also provides some observations drawn from primary research regarding AI adoption in EMDE financial sectors.

**This report is based on primary research comprising both a survey of EMDE authorities and selected in-depth interviews with financial sector authorities in both EMDEs and AEs.**

Responses were collected from 17 financial sector authorities from Africa and 10 authorities from other EMDE economies (generally referred to in this report as the ‘survey respondents’ or ‘surveyed authorities’). Additionally, interviews were conducted with several survey respondents and with a few authorities from AEs (see Annex).



# AI ADOPTION BY THE FINANCIAL SECTOR



## 2.1 Current state of AI adoption

**Digitalization has reshaped the financial sector, and AI has been playing an increasingly important role, with important implications for financial supervision.** The 1990s saw major advancements in ML, including its adoption in the financial sector. In the 2010s deep learning techniques gained further momentum and began to be applied in the financial sector, among other areas (Crisanto et al. 2024). In recent years, there has been an increased uptake of more powerful AI techniques, including by financial institutions (FSB 2024). As

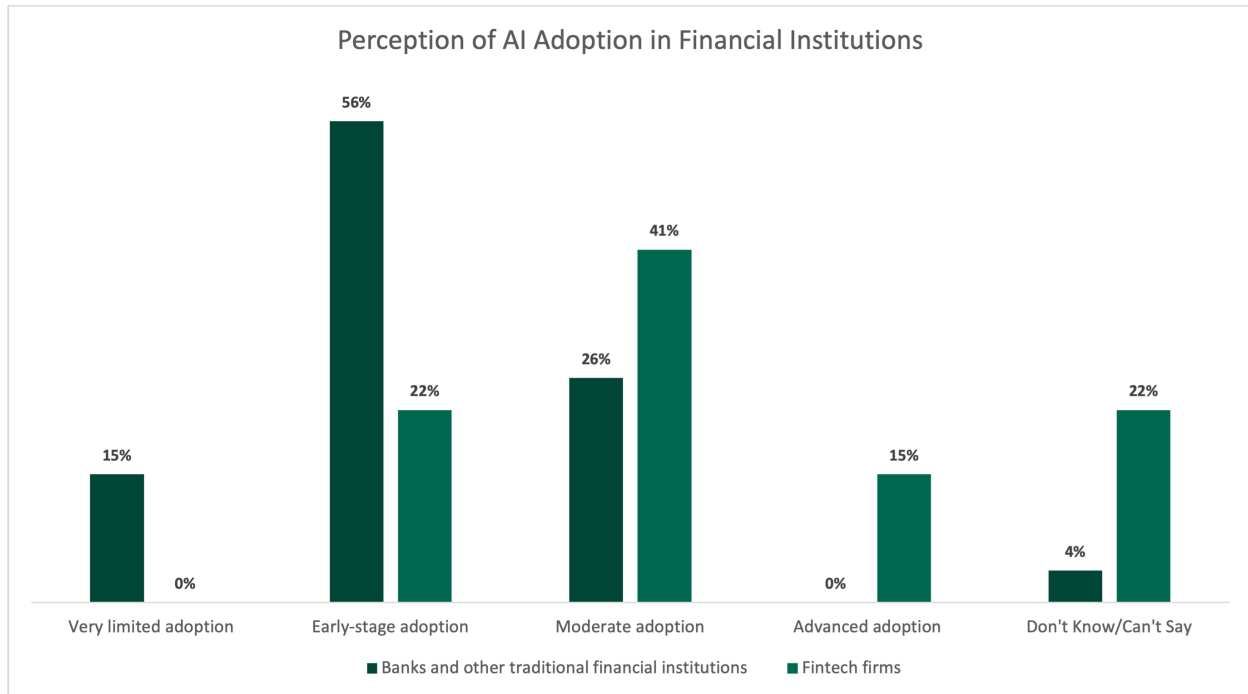
financial sector use cases have leveraged more advanced and complex tools and techniques, the usage of AI in finance has been shifting from rule-based automation to reliance on sophisticated data analysis, risk assessment, and predictive analytics to support decision-making processes and other tasks. It is estimated that by 2027 investment in software, hardware, and services for AI systems in the financial sector could reach \$400 billion, up from \$166 billion in 2023 (IMF 2023).

**The rapid adoption of technology, particularly AI, by the financial sector is reshaping the landscape of risks, prompting financial sector authorities to revise their approaches and assessments.** The rapid advancement of technology, combined with the increased availability of data for supervision purposes, has led to an exponential growth in the complexity and volume of data that supervisors must analyze. Furthermore, as financial institutions integrate AI into a wider range of activities, the landscape for supervisors could become even more complex. To maintain effective and robust oversight, authorities are modernizing their IT infrastructure—particularly in data collection, cleansing, and storage—and adopting SupTech tools, including by leveraging AI and other advanced analytics tools. At the same time, preparing for AI-related risks goes beyond technology. Laying the groundwork for risk-based supervision, reviewing existing supervisory practices, and employing market monitoring tools are vital for evaluating AI outcomes in the financial sector. These measures help to detect consumer harm and support swift supervisory and regulatory responses. By understanding the financial sector’s specific AI use cases, authorities can not only identify potential risks more effectively but also

discover new, relevant applications for SupTech. Importantly, authorities who are more experienced in the use of technology, including AI, can also leverage this knowledge to help them to better understand how well the industry manages its own technology-related risks. This parallel adoption is particularly relevant, for example, when considering specific risk areas such as financial consumer protection supervision.

**Non-traditional financial institutions such as fintech firms appear to take the lead in AI adoption in EMDEs, with traditional institutions following gradually.** Surveyed authorities’ perceptions are that fintech firms in their jurisdictions are more advanced in their AI adoption compared to banks and other traditional financial institutions. Most authorities saw fintech firms as falling into the moderate-to-advanced stages of AI adoption, whereas traditional financial institutions were seen as largely being at the very limited to early stages of AI use (Figure 2.1). Indeed, fintechs are generally already digitalized, while traditional institutions often face challenges linked to legacy infrastructure and more extensive regulatory and compliance requirements.

**Figure 2.1:** Traditional financial institutions are typically viewed as less advanced in adopting AI than fintech companies (n=27)



Question - "How would you describe the current adoption of AI by financial institutions in your jurisdiction? Respond separately for banks/ traditional financial institutions and fintech firms within your regulatory perimeter."

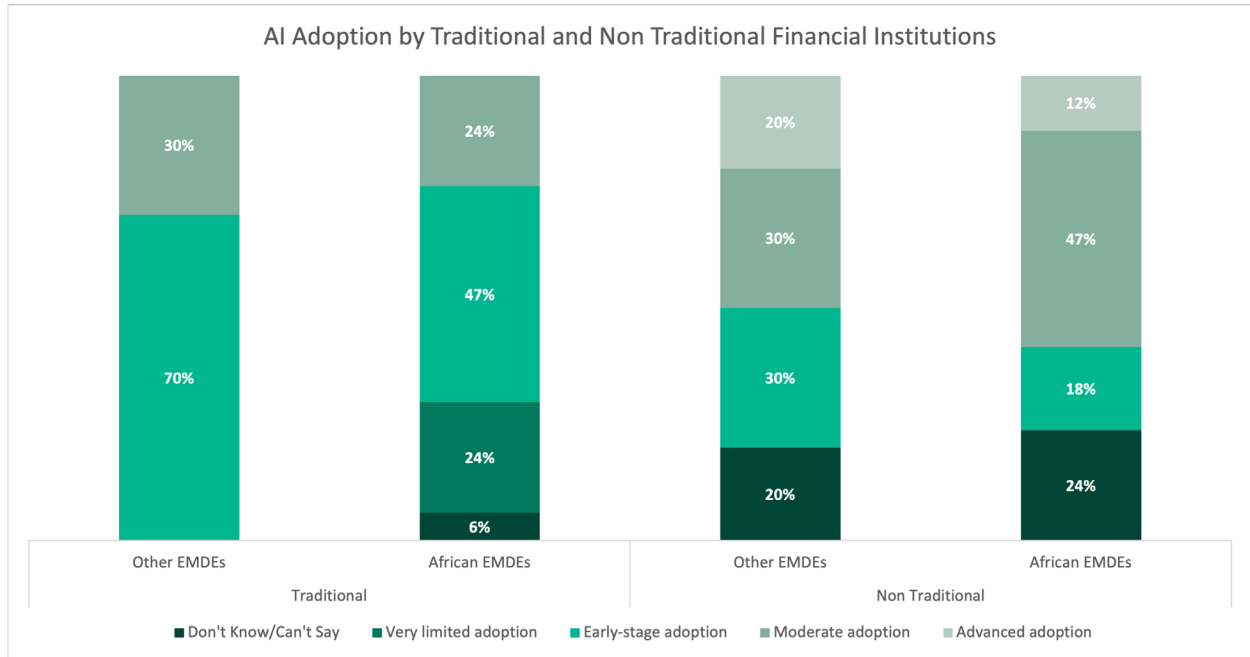
Note: Percentages may not total a hundred percent due to rounding.

Source: World Bank Survey on AI in Supervision, 2025.

**The adoption gap between traditional financial institutions and fintech firms identified by surveyed authorities is also wider between African and other EMDE counterparts.** When it comes to fintechs, African and other EMDE authorities are largely on par in their perceptions of AI adoption, with 59 percent of African survey respondents reporting moderate to advanced adoption, compared to 50 percent of respondents from other EMDEs. However, traditional financial

institutions in Africa show comparatively lower levels of AI adoption. While all other EMDE respondents reported early-stage to moderate AI adoption for traditional institutions, only 71 percent of African EMDE respondents reported similar levels and 24 percent indicated very limited adoption (Figure 2.2).

**Figure 2.2:** Traditional financial institutions are perceived to have lower AI adoption levels compared to non-tradition firms such as fintechs (n= 27)



Question - “How would you describe the current adoption of AI by financial institutions in your jurisdiction? Respond separately for banks/ traditional financial institutions and fintech firms within your regulatory perimeter.”

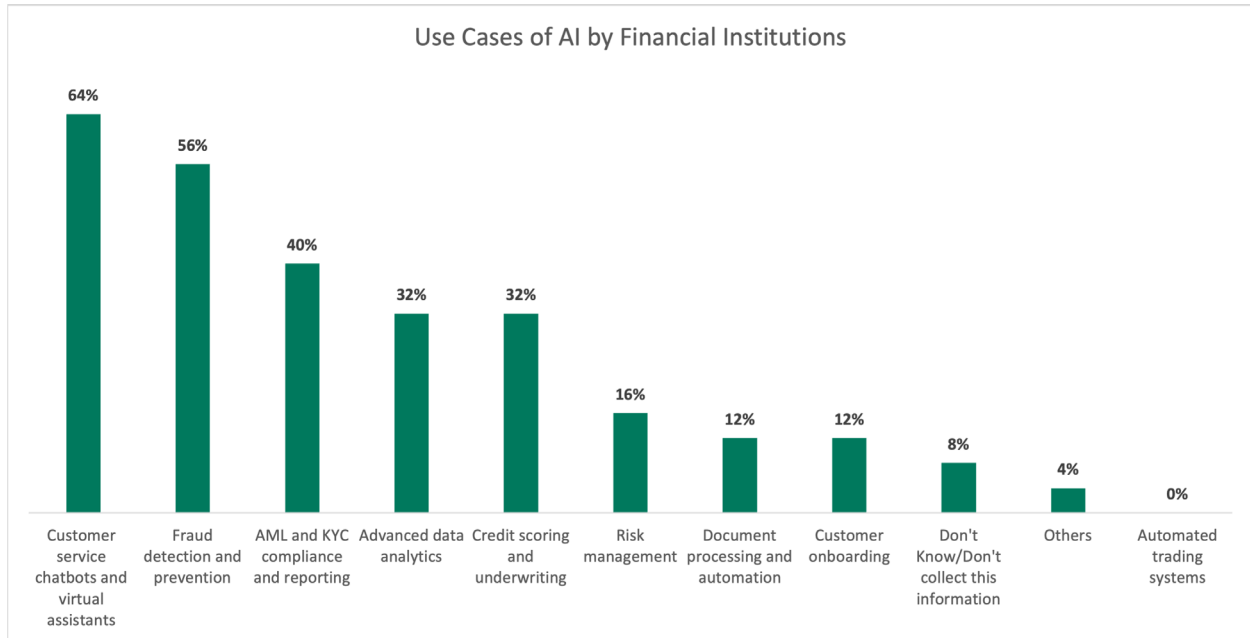
Note: Percentages may not add to a total of 100 percent due to rounding.

Source: World Bank Survey on AI in Supervision, 2025.

**Regardless of the level of AI adoption by financial institutions, there are some commonly reported financial sector use cases of AI.** Among surveyed authorities that reported at least an early level of AI adoption within their jurisdictions, the most common applications were in customer service chatbots and virtual assistants (64 percent), fraud detection (56 percent), and anti-money laundering and countering the financing of terrorism (AML/CFT) and know your customer (KYC) compliance and reporting (40 percent). The advent of GenAI has led to the rise of chatbots that can facilitate

more complex customer interactions to improve customer retention while saving costs. Additionally, the drive to improve regulatory compliance and meet requirements more efficiently is another key factor that is promoting AI adoption (FSB 2024). Notably, among financial institutions in African countries, credit scoring and underwriting are the second most common use case of AI. This may be partly due to a significant proportion of the population lacking formal credit histories, prompting financial institutions to use AI and alternative data to bridge the gap.

**Figure 2.3:** In jurisdictions with AI adoption, financial institutions most commonly use AI for fraud detection, customer service, and AML/CFT and KYC compliance (n=25)



Question - "What are the top three use cases of AI by financial institutions in your jurisdiction?"

Note: Only respondents who reported early stage, moderate or advanced levels of adoption by at least one type of financial institution were asked this question. This question was skipped for those who reported very limited adoption or did not know the level of adoption in their jurisdictions. Therefore, the total number of respondents is 25.

Source: World Bank Survey on AI in Supervision, 2025.

**The impact and pace of GenAI adoption by the financial sector is still to be assessed by most authorities.** EMDE authorities broadly indicated that they require further data and monitoring capacity to better assess their supervised entities' current status regarding AI. Given how GenAI has been increasing the pace of AI adoption, this may further increase the existing gap in risk

monitoring. Many financial institutions currently appear to be taking a prudent, risk-based approach to incorporating GenAI in business activities (FSB 2024). However, increases in AI accessibility and competitive pressures could facilitate a more rapid deployment than is currently reported, potentially with higher risks.

## 2.2 Outlook

---

**Most authorities, including those with limited or early-stage AI adoption, anticipate a net positive impact from AI in the financial sector over the next five years in terms of efficiency, competition, and inclusion.** While 59 percent of the survey respondents expect the impact to be ‘somewhat positive’, only 33 percent expressed greater confidence that AI would have a ‘very positive’ impact. Nevertheless, authorities who have identified financial institutions within their jurisdictions as being at a more advanced level of adoption have expressed a more positive stance about the future benefits of AI.

The increased pace of AI adoption by the financial sector also demands faster adaptation by financial sector authorities. It is important for authorities to develop a clear understanding of the technologies and governance frameworks adopted by financial institutions, as deficiencies in these areas may pose risks to the stability of these institutions and could also elevate risks to consumers. Many EMDE jurisdictions are taking proactive steps to engage with the financial sector on AI integration. Over half are seeking to support innovation through regulatory sandboxes, while a similar proportion are engaging in information exchanges with the industry on AI. A third have issued formal regulations or guidance. Interviewed authorities acknowledge the importance of supervisors being able to develop or enhance their ability to understand and assess AI-related risks, and

that use of AI in their supervisory activities could contribute to building understanding and expertise (also see Section 3).

At the same time, nearly half of the surveyed authorities indicated that they lack adequate systems, resources, and processes to monitor AI developments and assess their impact on financial institutions and consumers. This gap is more pronounced among African respondents (Figure 2.4). When asked whether they have sufficient systems, resources, and processes in place to monitor and understand the ongoing evolution of AI adoption in financial institutions, along with its associated impacts and risks, 53 percent of African survey respondents disagreed, compared to only 40 percent of the other EMDE respondents. None of the survey respondents strongly agreed that they are ready to monitor and understand the ongoing evolution of AI adoption by financial institutions, along with its associated impacts and risks. These findings are consistent with the limited readiness more broadly of financial sector authorities to deal with AI-related risks (World Bank, forthcoming). This can be contrasted with financial sector authorities in AEs and some technologically more advanced EMDEs that are already issuing guidance on AI model risk management for the financial sector (for example, Japan,<sup>3</sup> the United Kingdom,<sup>4</sup> and the United Arab Emirates<sup>5</sup>).

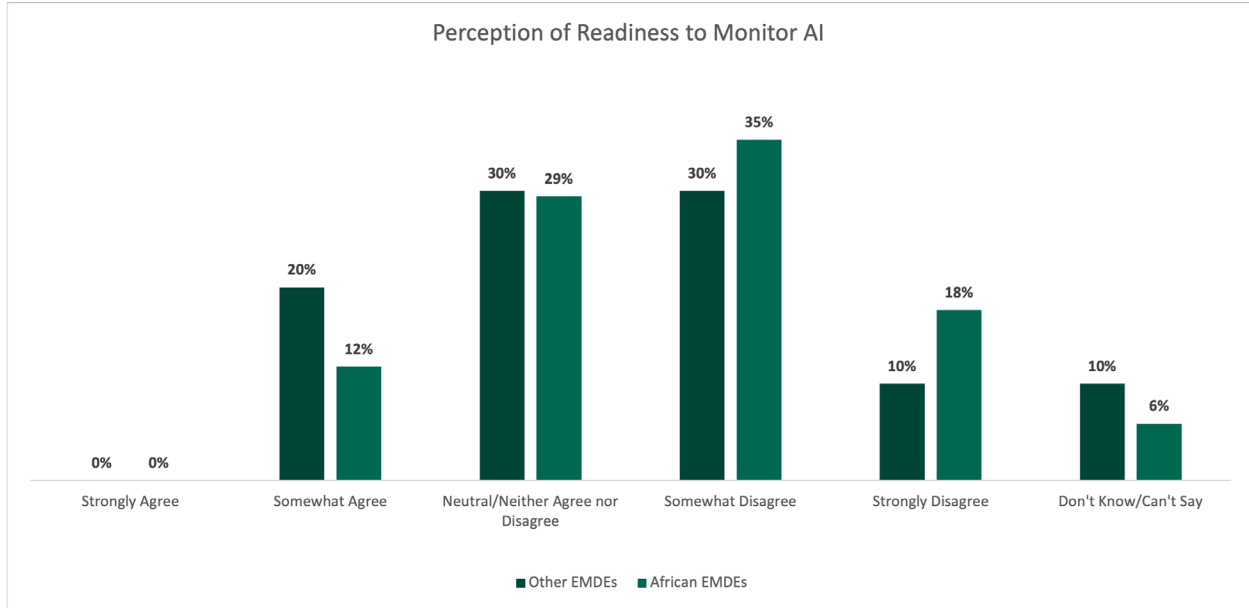
---

3. See Principles for Model Risk Management dated November 12, 2021 (Financial Services Agency of Japan)

4. See SS1/23 – Model risk management principles for banks dated May 17, 2023 (Bank of England)

5. See Model Management Standards dated November 2022 (Central Bank of the U.A.E)

**Figure 2.4:** Almost half of authorities reported lacking sufficient systems, resources, and processes to monitor AI developments and their impacts (n = 27)



Question - “My authority currently has sufficient systems, resources, and processes in place to monitor and understand the ongoing evolution of AI adoption in financial institutions as well as the associated impacts, including risks, on both the financial sector and consumers.”

Source: World Bank Survey on AI in Supervision, 2025.



## AI ADOPTION BY FINANCIAL SECTOR AUTHORITIES



### 3.1 Current state of AI adoption and outlook

**Several financial sector authorities have been exploring and developing ways to incorporate AI into their supervisory processes for many years, well before the advent of GenAI and agentic AI.<sup>6</sup>** ML algorithms, automated data analysis, and natural language processing (NLP) for document analysis and processing are examples of use cases that have already been deployed (e.g., Dohotaru et al. 2025), mostly by more experienced and better resourced authorities.

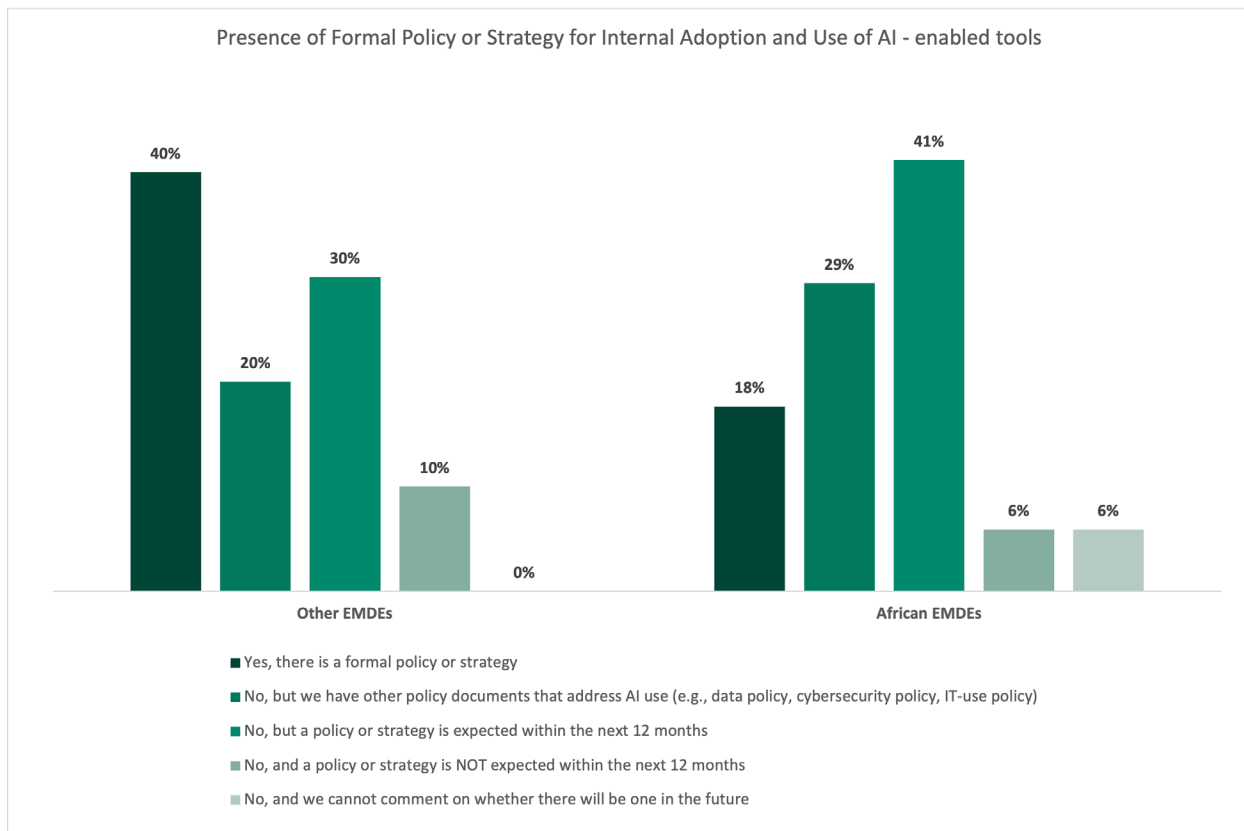
**However, GenAI can provide a basis to develop a range of new and more powerful tools for supervision.** Authorities who indicated that they had previously done very little with AI were also lagging in exploring use cases for newer forms of AI. In contrast, those that had been actively working on potential AI use cases for five or more years appeared better positioned to develop use cases for GenAI and even agentic AI.

6. The term agentic AI refers to computer systems which employ AI agents. An (AI) agent is a system with a relatively high degree of agency, Aldasoro et al. (2024). In the context of AI, the term agency can be defined as “the degree to which an AI system acts directly in the world to achieve long-horizon goals, with little human intervention or specification of how to do so, Chan et al. (2024).

**Authorities across EMDEs have recently started to adopt formal policies and strategies regarding their internal use of AI.** Twenty-six percent of surveyed authorities reported having a formal policy governing their internal use of AI, compared to only 18 percent of African authorities. Most

survey respondents that did not already have a formal strategy or policy expected to establish one within the following 12 months. Among African survey respondents, 41 percent indicated that they did not have a policy but intend to adopt one in the next 12 months.

**Figure 3.1:** Most respondents have, or will soon have, an AI use policy or strategy (n=27)



Question - "Does your authority have a specific formal policy or strategy on internal adoption and use of AI-enabled tools?"  
Source: World Bank Survey on AI in Supervision, 2025.

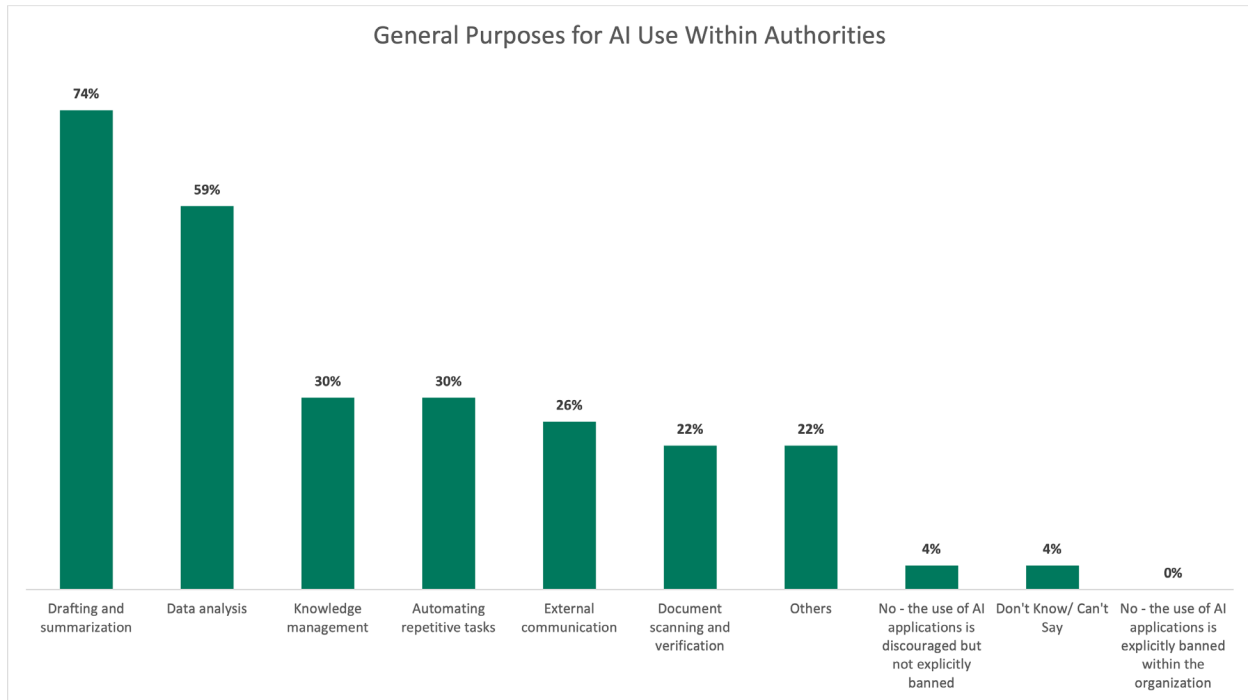
**Basic GenAI tools have seen widespread uptake by staff at authorities, both for supervision and other general purposes such as drafting and summarization.** Seventy-four percent of survey respondents indicated that their staff already use GenAI to some extent. Interviews confirmed that authorities largely view GenAI adoption as inevitable, with a need to have proper internal

requirements and guidelines in place for their use in supervision. Using AI tools for data analysis, while indicated as the second most common type of use case, appears to have room to grow within African authorities when compared to other EMDE authorities (47 percent versus 80 percent). While AI tools for drafting and summarization tools may be more readily useable, making tools available for

data analysis tends to require more preparatory work, both in designing and implementing appropriate requirements and collecting and preparing relevant data. For instance, it may be relatively easier for an authority to set up LLMs

for knowledge management and inquiries, and make them widely available for internal use than to develop a tailored anomaly detection tool for payment systems.

**Figure 3.2:** Most authorities use AI for drafting, summarizing, and data analysis (n=27)



Question - "For what general purposes are staff within your authority already using AI-enabled tools? Please consider the work of all department, including human resources, legal, procurement, research, and operation functions."

Source: World Bank Survey on AI in Supervision, 2025.

**In response to rapid changes in their business environments, financial authorities are seeking ways to systematize the adoption of AI in supervisory activities, while at the same time effectively managing the associated risks.** This requires working on both aligning AI adoption with organizational strategy and objectives to enhance efficiency and foster innovation, while maintaining robust risk mitigation measures through effective governance. This can result in complex internal tensions that need to be managed adequately (Consultative Group on Risk Management 2025).

Effective governance goes beyond issuing internal guidance or rules. It requires implementing clear decision-making structures, accountability mechanisms, and regular evaluation of AI tools and their impact on supervisory activities and the broader organization.

**In defining their strategies or/for establishing an AI governance framework, authorities have adopted a wide range of approaches and are aware of the need for internal policies to govern the use of AI.** While some interviewed authorities indicated

a preference to centralize the decision-making process on AI use case design and implementation, others have allowed individual departments to explore potential alternatives and consider in-house or outsourced solutions. Nevertheless, there is a consensus about the need for some degree of centralized oversight of AI applications within authorities, particularly during the development and initial adoption phases. Mechanisms being used for this purpose include, for example, internal committees and working groups. Some authorities have chosen to implement GenAI-specific policies, recognizing that these tools are typically externally sourced and therefore, require a higher level of governance and control. All interviewed authorities have developed or are working on AI governance and risk management frameworks.

**In the last few years, some EMDE authorities have been strengthening their IT and data infrastructures, including cloud computing, cybersecurity, and data warehousing aspects, as part of more general modernization processes.** Nevertheless, given the heavy reliance of AI on data, in some cases such a modernization may be driven or accelerated at least in part to enable AI adoption. Some authorities have opted to refrain from developing AI prototypes or proof-of-concepts (PoCs) until they are comfortable that their underlying infrastructure is sufficiently updated and well organized. For example, this has resulted in work on new and integrated databases, which—under this updated structure—can now be leveraged for the development of AI tools. Some

EMDE authorities noted that the use of AI tools for specific supervisory purposes such as forecasting, transaction monitoring, and scenario analysis (such as climate risk scenario analysis using geospatial data) is undertaken within specific departments and teams, and therefore institution-wide adoption has not been necessary at this stage.

**While most interviewed authorities see wide adoption of AI tools (especially GenAI tools) as a potential means to improve productivity while taking appropriate caution, many are also working to develop more specific AI tools for supervision.** Some interviewed authorities indicated that they are aiming for wide adoption of GenAI tools by staff but are also placing some restrictions on other specific AI tools. There are two main ways that authorities currently appear to be looking to incorporate GenAI into their work: i) staff using GenAI tools to support daily tasks and ii) the introduction of AI agents into formal workflows (also see Bell et al., 2025). Some authorities are exploring the use of agentic AI in supervision, in addition to other instances where AI may be embedded into supervisory processes. However, authorities indicate that these tools should complement, not replace, human judgment. Current limitations and risks relating to explainability, contextual understanding, and accountability highlight the need for human judgment to support effective and accountable financial sector oversight in the various supervisory domains (Perez-Cruz and Shin 2025).

## Box 1: Brazil

The Banco Central do Brasil (BCB) has been actively developing technology solutions for supervisory purposes that incorporate AI since 2018. Over this period, BCB has created approximately 40 proof of concept (PoC) projects, 10 of which have led to the development of solutions currently in production.

BCB has established a comprehensive governance framework for Cloud Computing and Software Strategy, which affects how AI is used in its activities. This framework is complemented by a specific set of internal guidelines, developed by the supervision departments, specifically for the use of AI in supervisory applications. For supervision purposes, the framework includes a dedicated committee responsible for coordinating the development of SupTech initiatives, supported by an office of technology and innovation. The committee, composed of representatives from key departments, is tasked with prioritizing initiatives and facilitating access to necessary data and personnel, thereby enhancing coordination across departments. For example, the use of cloud computing for AI-related data processing required BCB to update its regulatory framework to allow external data processing.

Within this governance structure, BCB's supervision departments are encouraged to experiment and develop their own PoCs, with technical support provided by the IT department. Supervising close to 1,900 entities, BCB has focused many of its AI solutions on increasing automation of data retrieval and enhancing analysis of internal data to streamline supervisors' workflows and enhance the quality of risk assessments. These tools are particularly valuable for monitoring entities with lower levels of inherent risk that may not be prioritized for ongoing or comprehensive inspections.

ADAM is an example of such a tool. ADAM examines the credit portfolio of supervised entities with the aim of helping supervisors identify credit exposures with potentially inadequate recognized expected losses (EL). The tool is capable of analyzing up to three million credit exposures, with the results of that analysis then subject to further consideration by relevant supervisors. AXIS is another operational tool developed to analyze independent auditors' reports. It uses LLMs to fully automate the capture of financial statements in PDF format, convert them to text, identify and extract reports, and perform specific regulatory tasks.

Given the breadth of its databases and applications and the internal demand for information, BCB is exploring the use of LLMs as a key component of internal chatbots. These chatbots aim to provide staff with easy access to both quantitative and qualitative data across BCB's systems, enabling more efficient responses to a wide range of queries. BCB has favored solutions that define a specific AI agent for each task, rather than broader agents covering multiple tasks, as this approach has proven more efficient. Furthermore, BCB is considering adapting solutions initially developed for specific purposes—such as analyzing complaints or consumer agreements—for use in other supervisory areas, such as AML/CFT or prudential supervision, subject to internal approval and prioritization.

Source: Summary of interview with BCB.

## 3.2 Current and future use of AI for supervision

**The adoption of AI for supervisory activities is a clear board-level priority for most survey respondents.** Seventy-five percent of survey respondents report that AI adoption for supervision is a board-level strategic priority. There is also a consensus that the potential benefits to authorities arising from AI adoption will outweigh the risks. However, survey respondents from Africa were more cautious in their attitude toward the risks-benefits tradeoff of AI compared to their other EMDE peers. Most of the survey respondents (59 percent) that are at a more advanced level of AI adoption within their institutions have a more favorable view of the potential benefits of AI.

**Nevertheless, most of the survey respondents describe their level of adoption as very limited or at early stages, which includes prototypes, pilots and/or sandboxes.** Only 11 percent of survey respondents report adoption of AI to support core supervisory functions (all outside Africa), while 37 percent indicate very limited or nonexistent adoption, and 48 percent report being at a very early stage of adoption. Notably, none of the African respondents indicate having adopted AI for core supervisory functions. However, all African authorities interviewed are developing a wide range of use cases, with plans for production deployment in the next 12 to 18 months.

**Advancing from experimentation to institutional adoption in a production environment is a critical step that many authorities find challenging.** Some authorities pointed out that even if prototypes show promise, they may lack the necessary data infrastructure, processing capacity, or human resources to adequately train these to a level sufficient for ongoing use. More recently, GenAI tools that are integrated into existing applications that are already in use by authorities have proven to be at least one feasible pathway for the use of AI solutions for many authorities, opening the way for

implementing more efficient ML tailored applications in future stages of development. The ability to skip the burdensome design and prototyping phases appears to be a clear incentive. Some applications of GenAI for supervisory purposes include recovery plans analysis, regulatory compliance verification, document processing, and analysis for in situ supervision, among others (Prenio, 2025). Interviews also highlighted that some authorities seemed to have made such tools available to all supervisory staff with relative autonomy in how they are used. Other authorities have been more cautious, limiting access of these tools to some supervisors, after careful screening and training, with close monitoring of potential impacts and results. Despite some steps taken to adopt GenAI, survey respondents are near-unanimous in their concerns about the use of public or non-corporate-approved and certified GenAI tools, given the high levels of confidential and sensitive data used by supervisory teams. GenAI is not necessarily the most appropriate option for all supervisory areas where AI may assist. Authorities may thus need to explore other types of AI solutions that are not necessarily as readily deployable.

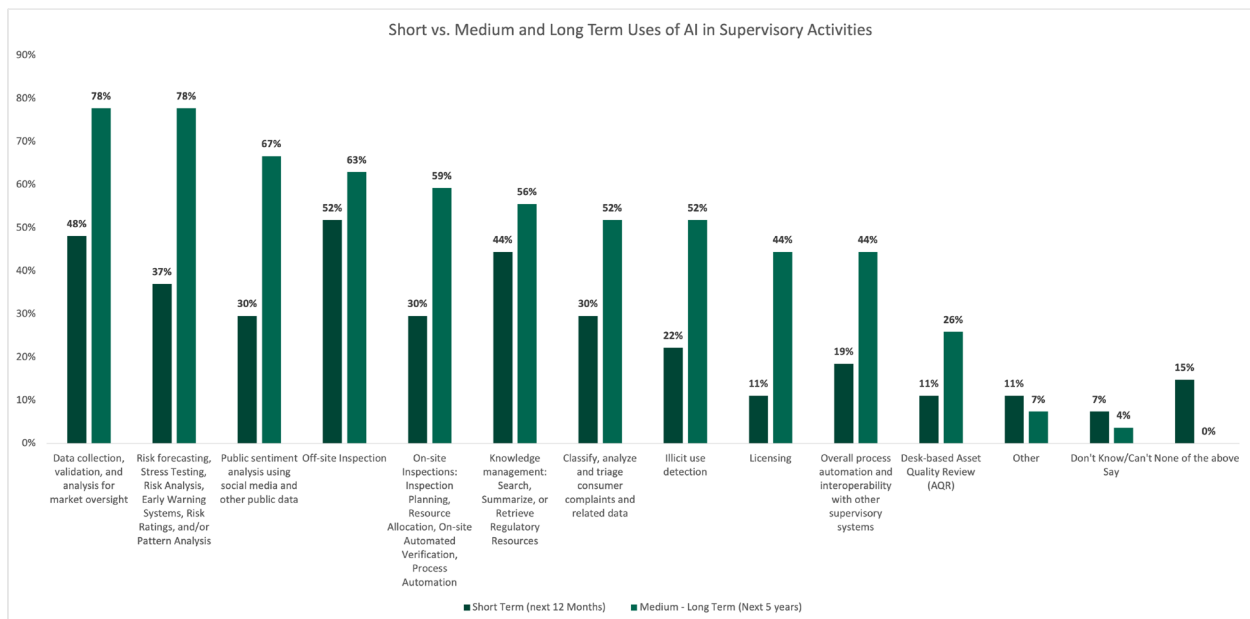
**Authorities are already using or planning to use AI for several supervisory areas, including activities such as micro-prudential supervision (48 percent), market conduct supervision/financial consumer protection (41 percent), and AML/CFT monitoring and supervision (44 percent).** Macro-prudential supervision and automation of licensing and authorization (both with 30 percent) and oversight of payments system (26 percent) are less frequently mentioned, with the latter being expressed only by African survey respondents.

**Supervisory activities that authorities indicate could benefit from AI in the next 12 months include off-site inspections, followed by data**

**collection, validation of data, and analysis for market oversight and adoption is likely to grow across most supervisory tasks over the next five years.** When asked about AI use in the next five years, 78 percent of survey respondents indicated data collection as a potential use case, and the same share (78 percent) pointed to risk forecasting, followed by public sentiment analysis (67 percent), off-site inspections (63 percent), and on-site inspections (59 percent) (Figure 3.3). Overall, this

indicates optimism of AI use cases for supervisory activities that are not currently in use. While there is generally a significant gap between short- and longer-term perspective of AI use across most supervisory activities, respondents are optimistic about the future use of AI for risk forecasting activities and on-site inspections. The potential for AI adoption in both knowledge management and off-site inspections appears to be more modest.

**Figure 3.3:** AI adoption by authorities is likely to increase significantly in the medium to longer term across a wide range of supervisory tasks (n = 27)



Question -“For which supervisory activities is your authority currently using or planning to use AI in the next 12 months? Select all that apply” and “For which type of supervisory activities will AI most likely be used in your authority in the medium to longer term (e.g., the next 5 years)? Select all that apply.”  
Source: World Bank Survey on AI in Supervision, 2025.

**In terms of which tools are being developed for internal knowledge management, some authorities have deployed or are deploying in-house LLM tools, AI agents, and chatbots.** For example, interviews suggest that authorities are increasingly opting to focus efforts on chatbots designed to answer queries based on internal data sources, including supervision manuals, regulatory

repositories, and databases of procedures. Some authorities are also using LLMs to develop a supervisory knowledge repository. In some cases, authorities are developing a separate dedicated AI agent to search and analyze each type of information or data source, which can facilitate more effective training and deployment. These multiple agents may then be queried by supervisors through one

chatbot, responsible for receiving the queries and routing them to the appropriate agent. Several authorities also expressed an intention to explore deploying AI agents to undertake other specialized tasks for supervision, including risk assessments, asset quality reviews, and complaints analyses.

**The adoption of AI for supervision often requires specialized skills that may not be readily present within authorities. Interviewed authorities indicated concern regarding the challenge of ensuring and maintaining updated skill sets in the near future.** This is especially important because authorities need to build an internal understanding of AI's risks and benefits for their organizations and activities even—and sometimes perhaps even more so—when relying on external vendors. Most interviewed authorities agreed that there is a need for a multidisciplinary approach to building internal capacity if they are to advance meaningful AI adoption. This often requires bringing together IT specialists, data scientists, and supervisors to co-develop AI tools that are not only technically sound but also operationally relevant and effective. One authority noted that they are embedding data scientists and technology specialists within supervisory teams to facilitate knowledge transfer: supervisors gain relevant technical insights while data and technology experts acquire the supervisory domain context needed to understand

operational needs and likely use cases. Authorities are training existing staff to help identify use cases and aid them in exercising effective judgment when working with AI.

**Authorities typically appear to rely on a combination of in-house development and external acquisition of AI models and tools.** For example, some EMDE authorities are developing their own ML models for analysis of specific regulatory data, pattern recognition, and anomaly detection (for example, spikes in transaction volumes). On the other hand, for GenAI tools, authorities tend to largely rely on off-the-shelf products (but allowing customization, whether by the authority or directly by users) or AI tools that are embedded into existing software applications already in use. However, at least one authority also mentioned that they are developing their own GenAI model using open-source code, while acknowledging that they were at the early stages. Across EMDEs and AEs, big-tech providers dominate the space for ready-made GenAI tools. In the long run, having fewer dominant AI technology providers could lead to the risk of market concentration and vendor lock-in (also see Sections 3.3 and 3.4). Additionally, AI application development increasingly relies on a highly concentrated market for accelerated computing chips, which could also further exacerbate concentration risks (FSB 2024).

## Box 2: South African authorities

South Africa's prudential and market conduct authorities, the Prudential Authority (PA) within the South African Reserve Bank, and the Financial Sector Conduct Authority (FSCA), have increased their internal focus on leveraging AI. They have been making efforts both on development of specific use cases to improve efficiency and effectiveness of particular activities, as well as on fostering responsible usage of GenAI by their supervisory and support staff more generally. In the case of both authorities, these initiatives are being undertaken within the context of enterprise-wide information and communication technology (ICT) frameworks that were developed or revised to incorporate AI-related considerations and plans.

Both the FSCA and the PA have taken deliberate and proactive steps to support the responsible adoption of GenAI by their staff. They identified relatively early a strong trend of staff wanting to leverage GenAI tools for their day-to-day work. The authorities appreciated that it would be difficult to 'stop the train.' At the same time, they were keen to address as quickly as possible potential risks, such as risk of exposure of sensitive data to external tools, that could come from usage of external unsanctioned tools. The PA has launched a PoC using commercially available GenAI large language model (LLM) for authorized use by staff. Both authorities are continuing their journey to expand access to AI tools while placing a strong emphasis on staff training, delivering such training in a variety of ways. Importantly, implementation of such tools comes with key safeguards such as restricting them to using sensitive data only locally and preventing external sharing of such data.

The authorities are also working on more specialized AI use cases. In the case of GenAI, for example, the authorities are working on implementing chatbots that can answer queries based on a wide range of internal data held by the authorities, as well as on public information (such as legislation), and which are intended to provide relevant and timely information that can speed up the work of supervisors and support staff. The FSCA has further plans to extend such a chatbot to external stakeholders in the near future. The training data for these tools includes data generated from manual work previously produced by staff such as, for example, previously answered email queries, etc.

The PA and FSCA have focused their efforts on progressing into full-scale production and deployment only with use cases that have proven to be both effective and sustainable.

Source: Summary of interview with FSCA and PA.

### 3.3 Challenges to AI adoption for supervision

**Integration of technology into supervisory processes is not without its challenges – and adoption of AI is no exception.** EMDE authorities rated the following as their top four key challenges to AI adoption: data privacy and security, internal skills gaps and workforce readiness, AI and model-specific challenges, and integration of AI into existing technology and processes (Figure 3.4).

Finding reliable SupTech providers and accessing high-quality data are also viewed as key barriers. One authority stated that their main challenge to adoption of AI was in coordinating efforts across a large economy with a complex regulatory structure and multiple regulatory authorities with different mandates

**Figure 3.4:** Data privacy and security, internal skills gaps, AI model-related challenges, and integration challenges are the top four barriers to AI adoption in supervision among survey respondents (n=27)

Challenges and Barriers	Overall rank	Score	No. of rankings
Data privacy and security	1	63	18
Internal skills gaps and workforce readiness	2	53	18
AI and model-specific challenges (training, validation, testing, transparency and explainability, governance and risk management)	3	50	14
Integration of AI-enabled tools with existing technology and processes	3	50	14
Finding reliable and context-appropriate SupTech technology providers	5	32	11
Accessing high-quality data	6	28	11

Question -“What are the top 5 (five) barriers and challenges to the adoption of AI-enabled solutions for supervision within your authority?”

Note: Survey respondents could select up to five challenges/ barriers from a larger set of options. The scores are the weighed scores for each challenge/ barrier out of a total possible score of 135—the top score would have been possible if all 27 respondents had selected the same option as the top option.

Source: World Bank Survey on AI in Supervision, 2025.

### 3.3.1 Skills gaps and workforce readiness

**EMDE authorities find that skills gaps and workforce readiness are key challenges to the adoption of AI within their institutions.** Authorities in African jurisdictions indicated that internal skills gaps and workforce readiness is a major barrier. Seventy one percent of African survey respondents identified it as a top five barrier. This can have various implications for internal AI adoption. For example, over half (52 percent) of authorities in African jurisdictions cited the lack of internal expertise to accurately assess vendor-provided AI tools as a key risk to adoption of AI (see Figure 3.5). Interviewees also mentioned challenges arising from a need for mindset change, addressing resistance to change, and changing institutional culture. Despite this, at least some interviewed authorities are actively working to address this skills gap, including by focusing on training existing workforces. Some

authorities mentioned they were actively hiring new talent, but the focus was largely on training existing staff.

**Hiring and retaining technological talent can often be a challenge for authorities.** Competition with the private sector for talent is significant in many EMDEs as talented and experienced technology professionals, particularly related to AI, are scarce (see Bell et al 2025). Some authorities also mentioned that lower salaries in the public sector as well as a perception of excess bureaucracy has made it harder to hire new tech professionals. This is not unique to AI, of course, although demand for AI talent may mean the challenge is even more acute in this context. Some EMDE and AE authorities are also trying to attract and retain technological talent through secondment programs as well as by highlighting the mission-driven, and public service focused nature of working for a government authority.

**Adoption of AI for some supervisory processes typically requires resources to be allocated for training, testing, and maintenance.** Just under half (13 out of 27) of survey respondents cited budget and resource constraints as a key challenge

to AI adoption. Several EMDE authorities stated in interviews that they were proactively hiring new technical professionals as well as training existing staff. A commonly referenced strategy to address the need for resources involves hiring or relocating

**Figure 3.5:** African authorities see internal skills gaps and integration of AI into existing technology and processes as top challenges (n=17)

Challenges and Barriers	Overall rank	Score	No. of rankings
Internal skills gaps and workforce readiness	1	37	12
Integration of AI-enabled tools with existing technology and processes	2	36	10
Data privacy and security	3	31	9
AI and model-specific challenges (training, validation, testing, transparency and explainability, governance and risk management)	4	29	9
Finding reliable and context-appropriate SupTech technology providers	5	25	9
Accessing high-quality data	6	23	8

Question -“What are the top 5 (five) barriers and challenges to the adoption of AI-enabled solutions for supervision within your authority?”

Note: Survey respondents could select up to five challenges/ barriers from a larger set of options. The scores are the weighed scores for each challenge/ barrier out of a total possible score of 85—the top score would have been possible if all 17 African survey respondents had selected the same option as the top option.

Source: World Bank Survey on AI in Supervision, 2025.

staff with technical and IT backgrounds and expertise to supervisory teams responsible for core supervisory activities. This is intended to balance traditional supervisory skills with new and evolving technological expertise.

### 3.3.2 Data quality and AI model training and validation

**Ensuring that AI models and algorithms are trained in a manner that is ‘fit for purpose’ is another challenge for authorities across EMDEs, with data-related limitations being a major factor.** A key aspect of this challenge for EMDE authorities is ensuring that AI models are trained on data that

is both high-quality and relevant to supervisory objectives. Authorities often face constraints due to limited access to digitized, structured data which hinders both the development and effective use of AI tools. Further, AI tools that are narrowly trained to identify only specific risks should not be expected to accurately identify other risks caused by factors that are not covered in the AI training data (Prenio 2024).

**The quality of the data used to train an AI model is a major determinant of model accuracy and usability.** Poor data quality is one of the most challenging aspects of AI model development and deployment. Poor quality data may comprise any

missing historical, unlabeled, biased, incomplete, noisy, untimely, inaccurate, or unadaptable data (Consultative Group on Risk Management 2025). It has been noted that to develop and train models and to test their efficacy, data should be clean, complete, standardized, and comprehensive (U.S. Department of the Treasury 2024). In EMDEs even more than in AEs, data is frequently still collected in unstructured documents or spreadsheets that may require data engineering and further preparatory work (even if itself AI-assisted – e.g., through analysis of PDFs) to maximize its usefulness for AI-related purposes.

**Lack of adequate data governance can also be a crucial barrier to effective AI adoption.** AI models often require large volumes of data, which can introduce governance challenges, such as those related to bias, accuracy, reliability, data tracking, security, and privacy. These may exist irrespective of whether authorities are using new data sources or repurposing existing ones. The nature, volume, variety, and quality of data used are all relevant considerations for effective data governance. The lack of structured, centralized data governance structures and processes in some jurisdictions might also lead to additional challenges in data governance (Cambridge Suptech Lab 2024).

### 3.3.3 Digitization and integrating AI into existing systems and processes

**Digitizing processes and the appropriate IT infrastructure, both prerequisites for the integration of AI, is a challenge for many authorities.** Survey respondents highlighted this difficulty in indicating that one of their top five challenges was integrating AI-enabled tools with existing technology and processes (see Figure 3.4). This includes adapting legacy infrastructure to new technologies and processes.

**Authorities may also face challenges in ensuring compatibility between new technologies and their legacy IT infrastructure.** Legacy IT environments

are frequently fragmented and characterized by siloed databases and outdated data architectures that were not designed to interact with modern AI-driven tools. New systems often require structured, high-quality, and interoperable data, while legacy systems may still rely on inconsistent formats, manual reporting templates, or isolated databases. Harmonizing these environments can be technically complex, resource-intensive, and time-consuming. In some cases, “leap frogging” by creating new systems and infrastructure might be more time and cost efficient than adapting existing systems.

**Authorities highlighted that AI use cases already in production are integrated into processes that were already well established and underpinned by reliable data.** For example, one authority developed an ML model to identify outliers in a monitoring process that was already in place for several years. Another created a chatbot designed to answer queries about a risk assessment methodology that had already been tested and piloted. However, it may pose greater challenges, especially for less experienced authorities, to seek to incorporate AI tools in less established processes. This can be the case, for example, for FCP/market conduct supervisors in EMDEs because this area of supervision is frequently recently established. In such cases, the more sensible preference may be to focus on relatively simple but repetitive tasks that can be more easily documented. For example, one EMDE mentioned testing GenAI agents to assist in analyzing inspection reports and other inspection documents. Complaints analysis was also mentioned, although it should be acknowledged that complaints data can be affected by significant data quality concerns, including due to its unstructured nature and diverse sources.

**Some of the interviewed authorities observed that piloting new and optional AI tools without making it a part of existing supervisory processes often resulted in low usage by staff.** This underscores the importance of not only introducing new

technologies but also aligning them with existing processes (including operating procedures) as well as with proven needs. Moreover, early experiments are essential for building internal expertise, testing viability, and driving innovation—especially in settings with limited resources. This emphasizes the need to develop clear pathways to expand successful pilots and embed them into formal supervisory workflows. As previously mentioned, one of the benefits for authorities of some ready-made GenAI tools appears to be that they can be more easily integrated into existing systems and processes, as their natural language interfaces can be integrated into reporting or case management systems with fewer adjustments, lowering adoption barriers. However, authorities must weigh the short-term benefits of rapid integration against longer-term requirements for reliability, security, and regulatory alignment.

### 3.3.4 Use of cloud infrastructure

#### **Cloud infrastructure can be important for widespread adoption of AI for various reasons.**

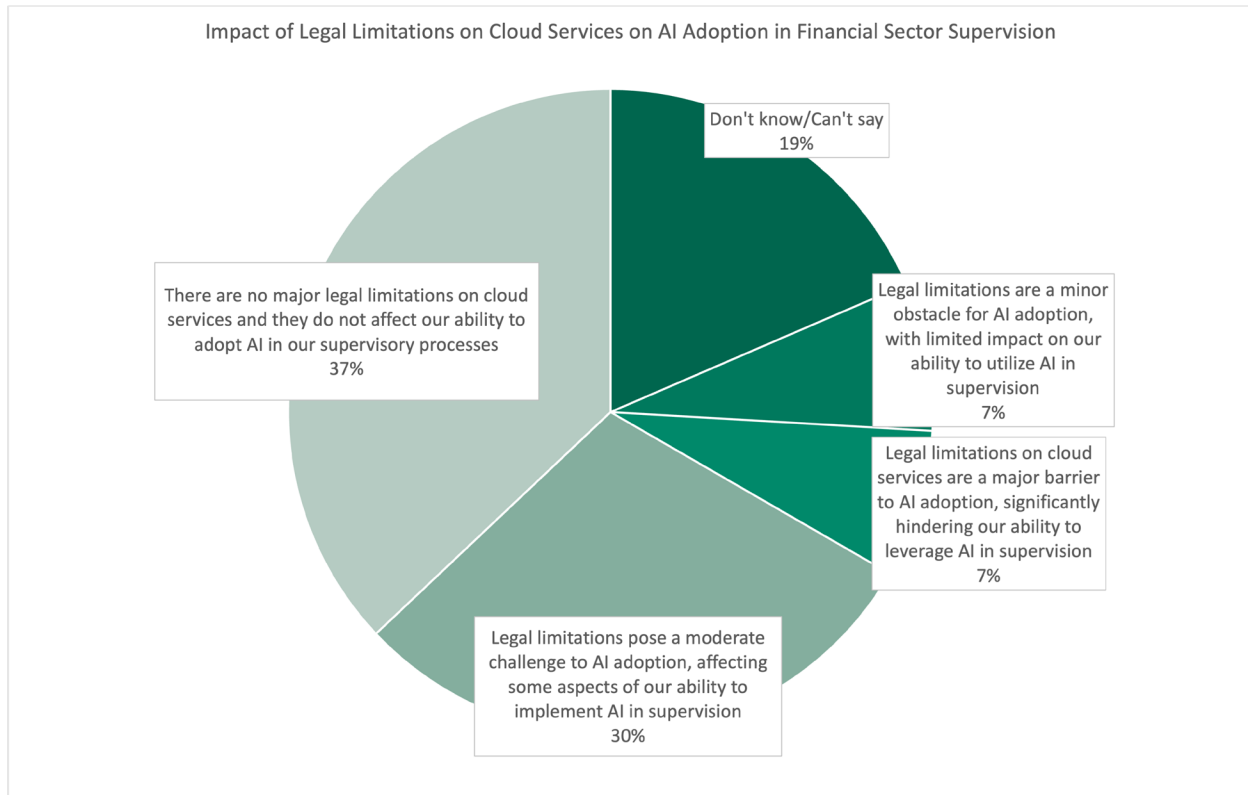
For instance, cloud infrastructure can be a means of accessing secure, scalable, and centralized data storage along with advanced tools for data integration, preprocessing, and governance. These are essential for training reliable and compliant AI models. Additionally, access to cloud services can

facilitate access to pre-built AI tools and models. Cloud-based systems can also facilitate intra- and inter-institutional collaboration.

#### **Some authorities have encountered challenges when transitioning their data to cloud-based systems.**

Thirty seven percent of survey respondents stated that legal and regulatory constraints on the use of cloud infrastructure were a major or moderate barrier to the use of AI. The same percentage responded that there were no barriers to the use of cloud infrastructure in their respective jurisdictions. One EMDE authority mentioned that their jurisdiction had to change regulations to enable the use of the cloud for data processing. For some EMDE authorities, having data stored and processed by external cloud service providers provided them with an opportunity to move from PoC phase to actual implementation of AI use cases. However, AEs are likely to face greater constraints on cloud use due to typically stricter data sovereignty and data security norms. It is also notable that most major cloud providers are big techs headquartered in a handful of countries. One interviewed authority suggested that cloud service providers may be compelled by their home governments to share information or disrupt or limit services, which may be a cause for concern to use such providers (also see Section 3.3.5 and Box 3).

**Figure 3.6:** Perceived obstacles to AI adoption due to local cloud service regulations vary significantly (n = 27)



Question –“How do legal limitations on cloud services impact authorities’ ability to adopt AI in financial sector supervision?”

Source: World Bank Survey on AI in Supervision, 2025.

### 3.3.5 Legal and regulatory challenges related to data privacy and security

**Some surveyed or interviewed EMDE authorities were concerned about the security of confidential supervisory data such as institution-level reports, transaction records, and consumer complaints.**

Additionally, AI models’ reliance on accessing large datasets and personal data of consumers may conflict with data privacy requirements for personal data to be erased on request. Some EMDE authorities indicated that these kinds of requirements can create practical challenges for AI-driven applications that need to retain data to function effectively. Restrictions are not necessarily limited to data privacy of individuals but may also be in force under confidentiality rules applicable

to financial services customers of any kind, or to the data about supervised entities. Some EMDE authorities mentioned that they are in the process of classifying data at more granular levels to clarify what data can be exposed to AI tools and what data cannot and should be kept confidential.

**Concerns around data localization and related data security risks have also prevented some authorities from exploring AI use cases.**

Some authorities indicated that it is crucial that their data reside within a specific physical region to avoid data sovereignty issues. For instance, one EMDE authority noted that they have not been able to fully explore the use of GenAI given such restrictions due to not knowing the exact location where the

data would be stored by the relevant cloud service provider. Several authorities indicated that they would be more comfortable with data being within their own jurisdiction – either on account of data localization rules or other data location concerns. Authorities face tradeoffs in deciding whether to enforce data localization: while doing so supports data sovereignty and governance, it may lead to performance issues, higher costs, and model bias (see Box 3).

**A risk-based approach may be helpful in such circumstances, even if it may not always be a complete solution.** For example, more stringent

requirements could be applied to more sensitive data. This approach can be operationalized by an authority through cloud encryption or a hybrid model, which involves storing highly sensitive supervisory datasets in sovereign cloud or local data centers while processing less sensitive data in commercial cloud environments to leverage scalability and advanced AI capabilities (World Bank 2024).

### **Box 3:** Key considerations related to cloud and data storage for adoption of AI by financial authorities

The adoption of AI by financial sector authorities can require a significant investment in IT infrastructure, including cloud computing and data related services. There are important considerations due to the high sensitivity of supervisory data. The following are some key aspects:

- **Data accessibility and quality:** AI can rely heavily on significant quantities of high-quality data for it to be successfully implemented. Some authorities face difficulties collecting, accessing, cleaning, and integrating such data. AI tools can be useful for precisely the purposes of data cleaning and transformation.
- **Outdated or deficient legacy data infrastructure:** Many authorities still rely at least in part on outdated storage and access data infrastructure.
- **Strict data governance frameworks:** Due to the confidential nature of data managed by authorities, restrictive data governance processes could limit the availability of useful data for AI models and tools.
- **Cybersecurity procedures and safeguards:** In the face of increasing and ever more sophisticated cybersecurity threats, stricter protocols have been implemented by authorities, including cloud computing services. This can make the implementation of AI solutions more difficult or at least more complex.
- **Data sovereignty and residency:** Requirements for retaining legal authority and control over data (data sovereignty) and/or physical storage and processing of data (data residency) can have significant implications when it comes to AI adoption that may require inconsistent arrangements.
- **Performance, costs, and bias:** Legal requirements that data must be stored and processed within a specific jurisdiction (data localization) could lead to reduced performance of AI models. Having to store and process supervisory data on specific jurisdictions could also lead to higher implementation costs and model bias.

### 3.4 Risks associated with AI adoption for supervision

**The use of AI tools for financial sector supervision can introduce or enhance several risks for authorities that can ultimately lead to performance issues and reputational risks, undermining public trust.** The top risks associated with the use of AI among survey respondents were data privacy and security, cybersecurity risks, lack of transparency in AI systems, operational risks including overreliance on AI and AI malfunction, vendor overreliance/concentration risks, and inaccurate model outputs (Figure 3.7).

**Despite these risks, authorities in EMDEs are generally optimistic about the potential benefits of AI in supervision.** For instance, 63 percent of

the survey respondents do not believe that the risks associated with AI outweigh the benefits, while only 11 percent (3 authorities in Africa) believe that it will. On a related note, as the financial sector rapidly adopts new technologies, authorities also need to modernize their own tools to keep up. In response to the pressure on financial sector authorities to update their technological infrastructure and tools, some commentators have suggested that these authorities should be given the opportunity to experiment—and possibly fail—as part of the innovation process, much like what is routinely accepted in the private sector (Allen 2023).

**Figure 3.7:** Authorities consider data security and privacy, cybersecurity, lack of transparency, and operational risks as the top risks associated with AI adoption in supervision (n=27)

Risk	Overall rank	Score	No. of rankings
Data security and privacy	1	71	18
Cybersecurity risks	2	69	16
Lack of transparency in AI systems (explainability or “black box” risks)	3	55	19
Operational risks due to overreliance on AI or malfunctioning of AI-enabled systems	4	42	13
Excessive reliance on third-party or external AI providers / Concentration risks	5	41	14
Inaccurate model outputs (e.g., hallucinations)	6	37	14

Question -“What are the top 5 (five) risks associated with the use of AI for supervision by your authority?”

Note: Survey respondents could select up to five risks from a larger set of options. The scores are the weighed scores for each risk out of a total possible score of 135—the top score would have been possible if all 27 survey respondents had selected the same option as the top option.

Source: World Bank Survey on AI in Supervision, 2025.

### 3.4.1 Data privacy and security

**Data privacy risks are of paramount concern to many EMDE authorities.** The risk of data breaches is elevated while implementing AI tools given the need for more extensive collection and retention of and access to sensitive data (Lopes et al. 2021). Supervisors across EMDEs are increasingly procuring internally operated GenAI applications for staff to prevent the use of public GenAI applications. While some early analysis had suggested that this option may not be cost-efficient for smaller institutions (see Shabsigh and Boukherouaa 2023), interviews suggest that the growing number of off-the-shelf tools created by big-tech firms appears to be making it easier for authorities to adopt institution-level GenAI applications that are embedded into existing software applications.

The effective use of AI applications might require an authority to migrate its data to a cloud-based environment, which can expose the authority to data security and other third-party risks. However, it can also offer significant efficiency and scalability benefits if data protection frameworks allow such access while safeguarding personal information (World Bank 2024). As discussed in the previous section, some of the interviewed authorities are wary of using cloud services due to data localization rules and third-party risks from technology providers, while several other authorities do not see it as a major concern. For instance, one EMDE authority expressed greater confidence in big-tech companies incorporated in jurisdictions where data privacy norms are perceived to be stronger than in their home jurisdiction. This gives them greater confidence in the provider's data privacy

and security practices. On the other hand, one authority in an AE cited concerns about losing data sovereignty due to using cloud service providers that are incorporated outside their jurisdiction. This concern was echoed by some EMDE authorities. Some authorities mentioned that they were looking to mitigate risks related to cloud use by adopting multi-cloud strategies or hybrid strategies where they did not solely rely on cloud infrastructure. One African authority decided to restrict AI usage to in-premise data storage and processing.

### 3.4.2 Cybersecurity

**Authorities' cybersecurity frameworks and policies may need further strengthening and adaptation to deal with new and enhanced risks due to AI tools.** AI applications often use large amounts of data, which may be subject to leakage or theft through cyberattacks or cybersecurity breaches. The pressure to rapidly adopt AI applications may lead to rushed implementations, increasing the probability of errors and/or exacerbating vulnerabilities that already exist (Consultative Group on Risk Management 2025). Among authorities in African EMDEs, cybersecurity risks were rated as the top risk to the adoption of AI (Figure 3.8). Robust cybersecurity governance, including national strategies, clear institutional mandates, and effective incident response frameworks, is essential for managing digital risks. While research shows that these measures are unevenly implemented across Africa, they are critical to mitigating potential cybersecurity vulnerabilities that could arise from the adoption of AI tools (World Bank, 2024).

**Figure 3.8:** African authorities consider cybersecurity, lack of transparency, and data security and privacy as top risks from the adoption of (n=17)

Risk	Overall rank	Score	No. of rankings
Cybersecurity risks	1	48	11
Lack of transparency in AI systems (explainability or “black box” risks)	2	37	13
Data security and privacy	3	35	10
Operational risks due to overreliance on AI or malfunctioning of AI-enabled systems	4	33	10
Excessive reliance on third-party of external AI providers / Concentration risks	5	26	10
Public trust in and reputational risks to the authority	6	21	6
Lack of internal expertise to critically assess vendor-provided AI tools	7	18	9

Question -“What are the top 5 (five) risks associated with the use of AI for supervision by your authority?”

Note: Survey respondents could select up to five risks from a larger set of options. The scores are the weighed scores for each risk out of a total possible score of 85—the top score would have been possible if all 17 African survey respondents had selected the same option as the top option.

Source: World Bank Survey on AI in Supervision, 2025.

### 3.4.3 AI model challenges

**Some AI models and the large datasets on which they are trained can be opaque.**

Transparency risks arise from the absence of public and detailed knowledge about the programming of AI models. These can also lead to governance and accountability issues due to a lack of understanding or inappropriate controls of databases and information used to train the algorithms of AI applications (Consultative Group on Risk Management 2025), as well as lack of a clear understanding of who bears the ultimate responsibility for AI-driven decisions. Consistent with these concerns, emerging principles such as the OECD AI Principles (2019, updated 2024), the U.S. National Institute of Standards and Technology’s Artificial Intelligence Risk Management Framework (2023) along with related guidance and updates, Principles for the Ethical Use of AI in the United

Nations System (2022), and the European Union’s Ethics Guidelines for Trustworthy AI (2019), all emphasize the need for robustness, transparency, explainability, fairness/ non-discrimination, security, and accountability in the deployment and use of AI.

**Lack of explainability or the “black box” nature of some AI models may exacerbate risks to supervisors due to difficulties in explaining outcomes or providing evidence on the reasoning behind a decision** (Consultative Group on Risk Management 2025. See also Perez-Cruz, F., Prenio, J. et al. 2025). While conventional statistical models produce well-defined parameters that experts can readily interpret, more sophisticated ML and AI models (e.g., neural networks) are less transparent. This concern is also reflected in the survey results, where lack of transparency in AI systems was the most selected risk among survey respondents (70

percent). It is of particular concern to authorities in Africa, as 76 percent of African respondents identified this as one of the top five risks. These AI-model risks might ultimately result in errors, data leaks, or lack of transparency, particularly due to inadequate control of complex AI models, and could hurt the reputation of the authority.

**Further, there is a risk of poor predictive performance from ill-designed algorithms, poor data or hallucinations from GenAI that supervisors might rely on to make decisions.**

Survey respondents from outside Africa, many of whom are actively looking at advanced use cases of AI, considered inaccurate AI model outputs to be among their top five risks. This risk is compounded by an inability to identify these inaccurate results in a timely manner due to model opaqueness. The risk of hallucination is especially significant when GenAI is utilized for document analysis or integrated into chatbot interfaces used by supervisory authorities. One of the AI industry experts and academics interviewed also added in this context that technology providers that create AI tools are often unable to explain how complex algorithms work and are therefore unable to preempt these risks.

**The potential for AI-based decisions to unintentionally perpetuate human biases and discrimination is also a concern.** A smaller subset of EMDE survey respondents indicated bias and discrimination as one of their top five perceived risks. A possible reason for this could be that many authorities are still in their initial stages of adopting AI in supervision and have not yet fully assessed the potential implications of such risks. Actors in more mature markets—both EMDE and AEs—appear to be more focused on the potential implications from bias and discrimination due to AI.

### 3.4.4 Operational risks

**The integration of AI into supervision may pose**

**operational risks, like those associated with the incorporation of any new technology into the supervisory process.** Such operational risks are wide-ranging, and many can be significant. From an IT perspective, in technologically interconnected systems, individual malfunctions can have cascading effects on the wider system. Additionally, in cases where supervisors begin to use certain AI tools widely for market monitoring or for assessing systemic risks, common regulatory blind spots could emerge due to overreliance on AI tools. Previously trained models might become outdated due to changing market conditions and regulatory frameworks, requiring the need for continuous monitoring and recalibration. In this context, one EMDE authority mentioned that their AI use cases in supervision are focused on microprocesses such as document summarization—including regulatory reports—and meeting minute taking. This strategy takes a cautious stance against the risk of large-scale operational errors or failures, given the current stage of AI adoption. However, such a strategy is only useful in the short term. A more comprehensive strategy is required to mitigate large-scale operational risks from the wider adoption of AI tools.

**Overreliance on any AI tool can lead to an inability among supervisory staff to perform their duties independently, even more so when it comes to less experienced supervisors.** Such concerns were mentioned by many interviewed authorities and experts. They noted that while AI could be a helpful tool for supervisors to carry out their supervisory responsibilities, maintaining independent supervisory judgment was crucial. It is imperative that supervisors are able to explain and justify their decisions both internally and externally. Overreliance on AI models might also hinder the development of institutional knowledge, critical analytical skills, and expertise, particularly in jurisdictions where supervision is not yet well-established or fully developed, or

---

7. For instance, market conduct supervision is a fledgling area of supervision in many EMDE jurisdictions, often characterized by a predominantly qualitative approach to risk assessment. Market conduct supervisors are often required to make subjective assessments as to whether a given business practice is unfair or if consumers are being treated fairly. In such cases, it is crucial to ensure that new or inexperienced supervisors are trained to make core judgments independently of AI models. Moreover, they must possess the capability to evaluate and critique decisions generated by AI systems.

where supervisory judgment is inherently more critical.<sup>7</sup> As noted by some experienced authorities, the testing and training of AI models has proven to be time-consuming and not entirely effective, indicating that even the most well-trained models remain prone to inaccurate outputs.

### 3.4.5 Vendor-related risks

**Determining which service provider or vendor can reliably deliver AI-based SupTech solutions is a significant consideration for many EMDE authorities when it comes to AI adoption.** An authority may need to rely heavily on a vendor for successful AI deployment, given limited internal capacity. Among African authorities surveyed, 53 percent of African respondents identified the lack of internal expertise to critically assess vendor-provided AI tools as one of the top barriers to the adoption of AI. Pressure from very limited budgets can also weigh heavily on such selections. The need for outsourcing may vary at every step of developing and deploying solutions. While some authorities may have sufficient capability to begin developing and testing AI models internally, this is rarely the case for less experienced ones which will consequently need to rely on vendors. For instance, an African authority opted to develop a customer-facing chatbot to be deployed on premises, thereby avoiding reliance on outsourced data storage and processing infrastructure. However, they chose to outsource the PoC development, citing a lack of the necessary expertise required for the task.

**Outsourcing can strain budgets and timelines due to the need for more structured contracts, oversight, and coordination with external vendors.** In contrast, in-house development, when possible, can offer greater flexibility. Outsourcing also presents challenges in defining appropriate procurement criteria for novel activities and for assessing the suitability of vendors with non-traditional profiles. On the one hand, the authorities interviewed have noted that outsourcing helps build

knowledge and capacity among their staff. On the other hand, it can lead to prototypes that are not adequately tailored for deployment in a production environment. This challenge underscores a key gap between AE authorities and those in EMDEs: EMDEs are more reliant on outsourcing and often have less time and flexibility to experiment and innovate.

**Even when an authority successfully selects a reliable and context-appropriate vendor, excess reliance on outside providers remains a concern.** Some EMDE and AE authorities indicated that they are seeking to address this challenge at least in part by developing proprietary in-house AI tools and capabilities. However, most noted that relying on big-tech companies to some degree was nearly inevitable given their vastly superior ability to handle and process large amounts of data. This is in line with the findings of the Cambridge Centre for Alternative Finance (CCAF)'s State of SupTech Report (Cambridge SupTech Lab 2024), which reveals a similar trend for adoption of SupTech applications generally across a cross section of jurisdictions. According to that survey report, both AEs (67 percent) and EMDEs (69 percent) demonstrated a strong focus on building in-house capabilities for SupTech solutions (Cambridge SupTech Lab 2024).

**Nevertheless, globally the reliance on specialized hardware, cloud services, and pre-trained models has increased the risk of third-party dependencies (FSB 2024).** In EMDEs, authorities may have access to an even more limited number of technology companies that can support their needs, which leads to concerns of vendor overreliance. If a contractual relationship with a vendor deteriorates, authorities may have limited options to find replacements given market concentration. A little over half of the survey respondents stated that vendor overreliance and concentration risks were a concern. However, interviews revealed that authorities in EMDEs and AEs tend to rely on big-tech AI providers, at least for GenAI solutions. One

factor is the lack of readily-available alternatives to big-tech providers for high quality AI models. Additionally, at least a part of this reliance on big-tech may be attributed to confidence in the stability and reliability of big-tech actors, as well as their perceived ability to comply with globally-accepted data privacy and cyber resilience standards. As already mentioned, some EMDE authorities perceive big-tech companies as more reliable in handling data privacy and cybersecurity risks.

**Authorities are developing contingency plans such as backup systems, should they need to switch vendors.** Some authorities are also ramping up internal capacity to manage the transition to new vendors if existing vendors are no longer suitable. Some of the interviewed authorities have also contractually agreed with their cloud service providers—including big-techs, in some cases—to expedite migration protocols. This has been done to maintain flexibility in selecting the best options and smoothly migrate to different platforms and

providers if deemed necessary.

**Vendor lock-in may occur, for example, when authorities implement opaque AI systems without the internal capacity to retrain or adapt AI models to new information, or without provision for source-code access and documentation.**

Good practices include ongoing capacity-building clauses for authorities' staff members, contingency plans, staged handovers, and co-development models in vendor contracts to reduce overreliance over time. Flexible procurement approaches (from prototype to pilot to scale-up) also allow authorities to experiment without prematurely committing to a single vendor. Vendor concentration risks are amplified where only a handful of providers dominate the AI cloud and hardware ecosystem, which underscores the importance of regional collaboration and cultivating local providers to diversify options.

### 3.5 AI governance and risk management

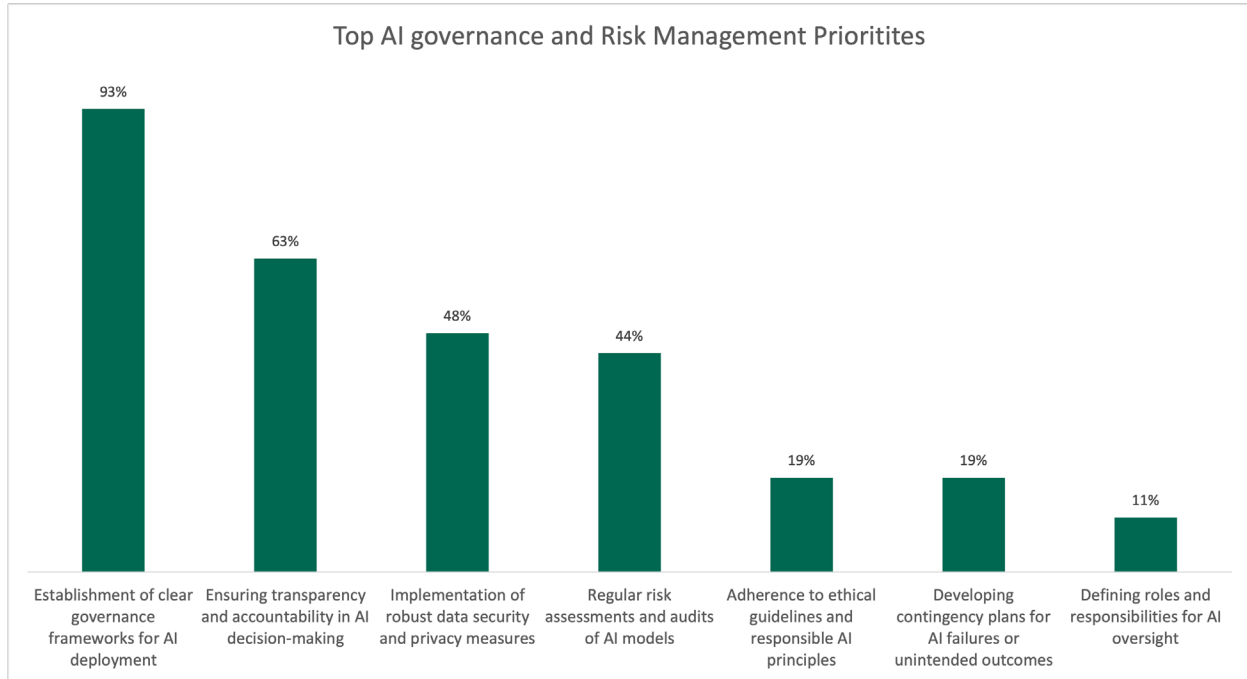
---

**Authorities across EMDEs have been exploring the issue of AI governance and risk management as AI use cases become more advanced.** There is a need to strike the right balance between promoting innovation and limiting the inherent risks that come with a widespread adoption of AI in the financial system as well as within their own organizations. Adequate, risk-based and up-to-date governance schemes are crucial to achieving such an objective (e.g., IFC 2024 and Consultative Group on Risk Management 2025). Moreover, strategic risk is among the most prominent types of risk associated with the adoption of AI for supervisory purposes (Bell et al. 2025).

**Establishing clear AI governance and risk management frameworks and ensuring transparency and accountability in AI decision-**

**making are key considerations for EMDE authorities.** Ninety-three percent of survey respondents stated that this was one of the top three priorities in AI governance. Sixty-three percent of survey respondents also noted that ensuring transparency and accountability in AI decision-making was a top three issue of importance when adopting AI in supervision. Additionally, 44 percent of survey respondents believe that regular risk assessments and audits of AI models are an important aspect of AI governance. These trends were consistent across African and other EMDEs that were surveyed. Interviewed authorities also emphasized the importance of guidance from senior leadership on how the adoption of AI should be undertaken.

**Figure 3.9:** Authorities are largely focused on establishing clear governance frameworks for AI deployment and ensuring transparency and accountability in AI decision making (n=27)



Question –“What are the top three AI governance and risk management aspects that are important for your authority when considering adopting AI in supervision?”

Source: World Bank Survey on AI in Supervision, 2025.

**AI governance frameworks can be built on existing policies, strategies, and risk management processes within the organization.** Authorities across EMDEs and AEs are taking various steps to adopt internal governance frameworks for AI use. Many research institutions and international organizations have adopted principles for governance and responsible use of AI, which can be used as a starting point by EMDE authorities.<sup>8</sup>

**Within this context, accountability and ownership of risk from AI use would encompass different dimensions.** An important one is that institutions developing, deploying, or operating AI systems should be accountable for their proper functioning and governance.<sup>9</sup> For financial sector authorities,

this also entails understanding and managing risks associated with the AI tools used and with third-party vendors involved in the AI lifecycle. Another relevant dimension is that supervisors should retain ultimate responsibility for justifying their supervisory decisions and for addressing potential risks and blind spots associated with the use of AI in decision-making processes. This underscores the need for a balanced and clearly defined allocation of responsibilities to ensure the trustworthy use of AI systems when designing governance frameworks.

8. These frameworks share common elements to implement AI processes that are robust, ethical, fair/ non-discriminatory, secure, transparent, explainable, reliable, responsible and comply with data privacy.

9. Consistent with OCED Principle 1.5.

#### Box 4: European Central Bank

Since initiating its digitalization strategy in 2020, the ECB has transitioned from tentative experimentation to building foundational infrastructures starting with unified databases, document repositories, and internal platforms, which are prerequisites for the systematic experimentation and large-scale deployment of AI tools. Several SupTech tools are already operational. Notable examples include Athena, which enables supervisors to search, summarize, and analyze confidential supervisory documents, and Delphi, which aggregates market and news data to create risk-based indicators for market-quoted banks. Another tool, Heimdall, accelerates the assessment of board member appointments by flagging potential risks within submitted questionnaires and CVs.

The ECB's strategic approach to AI adoption is marked by a blend of top-down vision and bottom-up innovation. The initial push originated from senior management, which articulated a clear digitalization blueprint and established a steering committee dedicated to innovation, while maintaining a strong focus on identifying and mitigating associated risks. The ECB has since invested in upskilling staff, raising awareness, and fostering a culture of openness toward technology, supported by partnerships with academic institutions and regular training for both management and staff. The ECB has also empowered interdisciplinary teams—comprising IT experts, supervisors, statisticians, and external consultants—to develop individual AI use cases as “start-ups within the organization.”

With the foundational infrastructure in place, the next phase will focus on scaling up successful pilot projects, refining use cases, expanding risk assessment capabilities, and empowering users. The aim is not to supplant human supervisory judgment with AI, but rather to harness AI's capabilities to free up expert time, enhance consistency, and raise the quality of supervision. An important lesson is the need to coordinate between multiple authorities and across national borders in Europe, especially given fast-evolving technologies, rapid AI adoption, and cross-border operations of supervised institutions.

Source: Summary of interview with ECB.

# 4 C

## AI-RELATED CONSUMER RISKS AND SUPERVISION

**Consumer risks stemming from financial sector adoption of AI are likely to continue to be an important focus for authorities, especially as financial sector AI use cases grow.** Such risks are of course highly relevant for authorities responsible for financial consumer protection and market conduct supervision, but they can also have other supervisory implications. Thus, as noted above, while the primary focus of this report is on adoption by authorities of AI for financial sector supervision, it has an additional albeit more limited focus on AI consumer risks. Given the focus of other reports on other important risk perspectives (e.g., prudential), this section explores how EMDE authorities are

engaging with consumer AI-related risks in the context of FCP/market conduct supervision. Adoption of AI for such supervision could also be useful in monitoring and analyzing such risks, including given their frequently qualitative rather than quantitative nature and the potentially disparate range of risk sources and scenarios.



## 4.1 Supervisory perceptions of consumer risks

### **Overall, fraud and scams are reported as the main concern from a consumer risks perspective.**

Most survey respondents (59 percent) view this risk as high for consumers (Figure 4.2) and a similar portion (Figure 4.3) consider supervising such risk very challenging. The level of concern relating to such risk is not surprising, given both global trends in the level of impact and sophistication of frauds and scams generally, whether or not relying on AI, as well as a range of incidents of frauds and scams that have already relied specifically on AI (see, for example, Heikkila 2024 and Barrett 2025, and OECD 2024).

### **The risk of fraud and scams to consumers, exacerbated by AI use and primarily driven by external actors, increases the challenge to be addressed from a supervisory perspective.**

In such cases, authorities' primary focus would thus need to be on the role of financial institutions in preventing and mitigating such external risk, and how consumers are treated fairly (or not) after being subject to such events (World Bank Group 2017). The potential impact of AI would be part of broader considerations, regarding not only supervision of relevant obligations on financial institutions, but also potentially implementing more comprehensive initiatives relating to fraud monitoring, prevention, and mitigation (see, for example, Renier et al. 2025). The potential of AI technology to detect AI-driven frauds should also be explored by authorities, evolving from traditional rule-based security systems. AI-powered fraud detection systems can help identify suspicious activities in real-time through anomaly detection and predictive analytics, reducing financial losses and enhancing security (see, for example, Chettier and Boyina 2025).

**Cybersecurity and data security and consumer privacy risks from AI are also of clear concern to authorities.** Nearly half of survey respondents

view such risks as high for consumers (48 percent and 44 percent respectively), with around a third more viewing these as at least medium risks (Figure 4.2). As with other risks highlighted here, the impact of such risks is of course not limited to consumers (see, for example, Crisanto et al. 2024). The cross-cutting nature of some of these risks beyond the financial sector also means financial sector authorities are having to consider how these fit within their sector-specific mandate and what cooperation may be needed with authorities that may be responsible for data protection, and increasingly for cybersecurity-related matters, across a whole jurisdiction (also see Section 5). For example, one African authority noted that both the national data protection authority and the national agency for information technology in their jurisdiction may have roles to play regarding AI uptake in the financial sector as part of their broader purview.

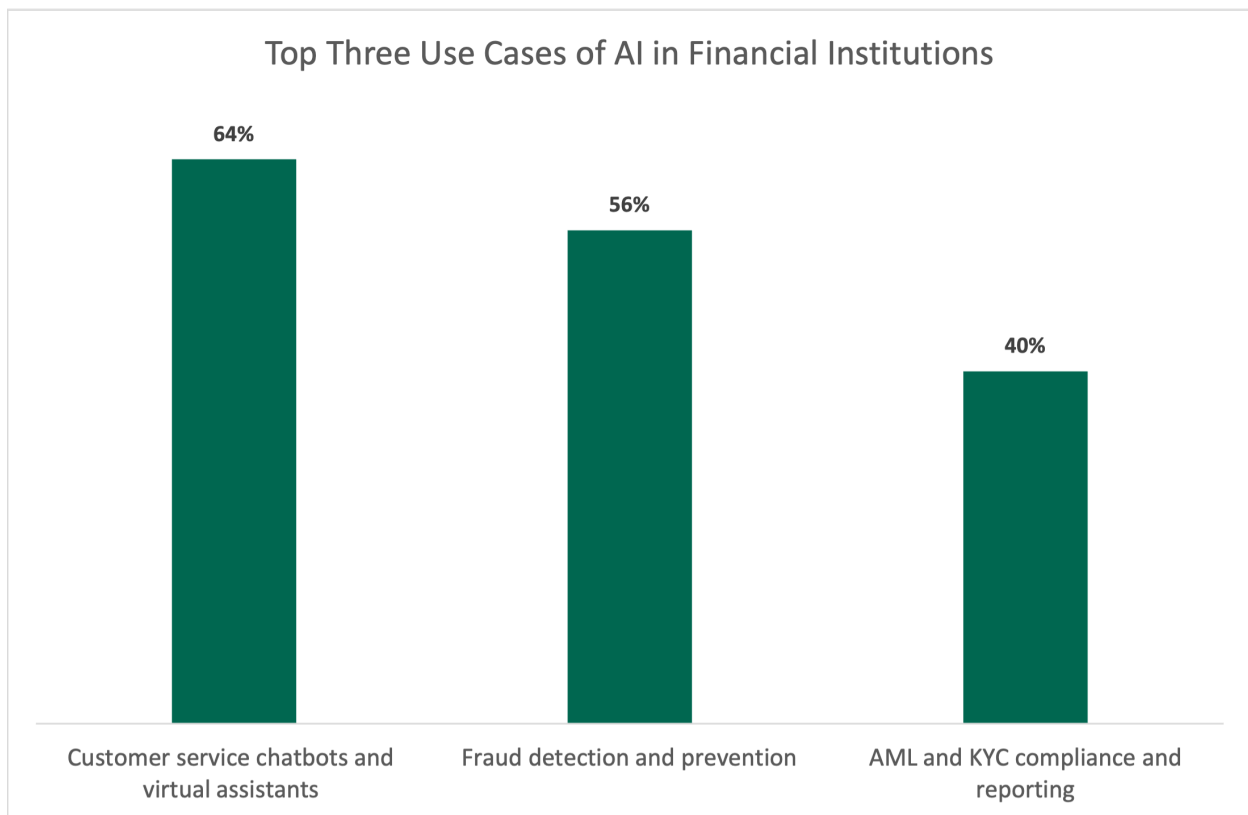
### **When it comes to other AI-related risks, many authorities appear to already recognize their potential significance for consumers, but others still find it difficult to determine the potential impact.**

While around a third of survey respondents viewed as a medium risk for consumers issues such as bias and discrimination, lack of explainability, lack of transparency, and manipulation of decision-making, around a quarter or more of survey respondents were unsure. This would obviously be affected by various factors, including the level of adoption of AI in financial institutions' dealings with consumers and the level of monitoring by, and understanding of, AI-related risks by authorities as part of their financial consumer protection supervision. Most authorities, especially from EMDEs, have expressed difficulties in clearly identifying or describing current risks arising from known specific use cases adopted by their supervised institutions.

**Increasing engagement with financial institutions’ implementation of AI use cases will be essential for authorities to have a better understanding of the source and nature of potential risks for consumers.** For example, both survey responses (Figure 4.1) and interviews with several authorities suggest the roll-out of consumer-facing chatbots by financial institutions to be a growing phenomenon to which authorities are paying some attention. The greater awareness

of such AI use by authorities may in part explain why over half of the authorities already view provision of inaccurate information as presenting a medium or higher-level risk for consumers (48 percent—medium, 15 percent—high) (Figure 4.2). The increasing experience that authorities referenced having gained internally with development of their own GenAI-based chatbots, including in seeking to address potential risks of ‘hallucination’ or other inaccuracies, may also have assisted with this.

**Figure 4.1:** Fraud detection and prevention, customer service chatbots, and AML and KYC compliance and reporting are the top three uses of AI in financial institutions (n=25)

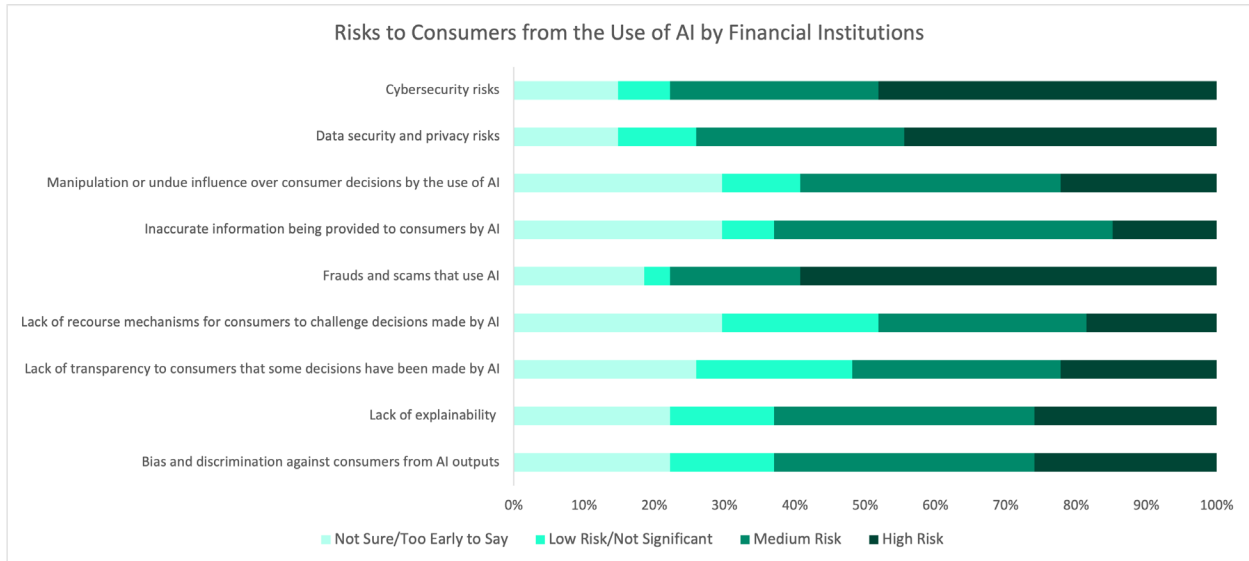


Question -“What are the top three use cases of AI by financial institutions in your jurisdiction?”

Note: Only respondents who reported early stage, moderate or advanced levels of adoption by at least one type of financial institution were asked this question. This question was skipped for those who reported very limited adoption or did not know the level of adoption in their jurisdictions. Therefore, the total number of respondents is 25.

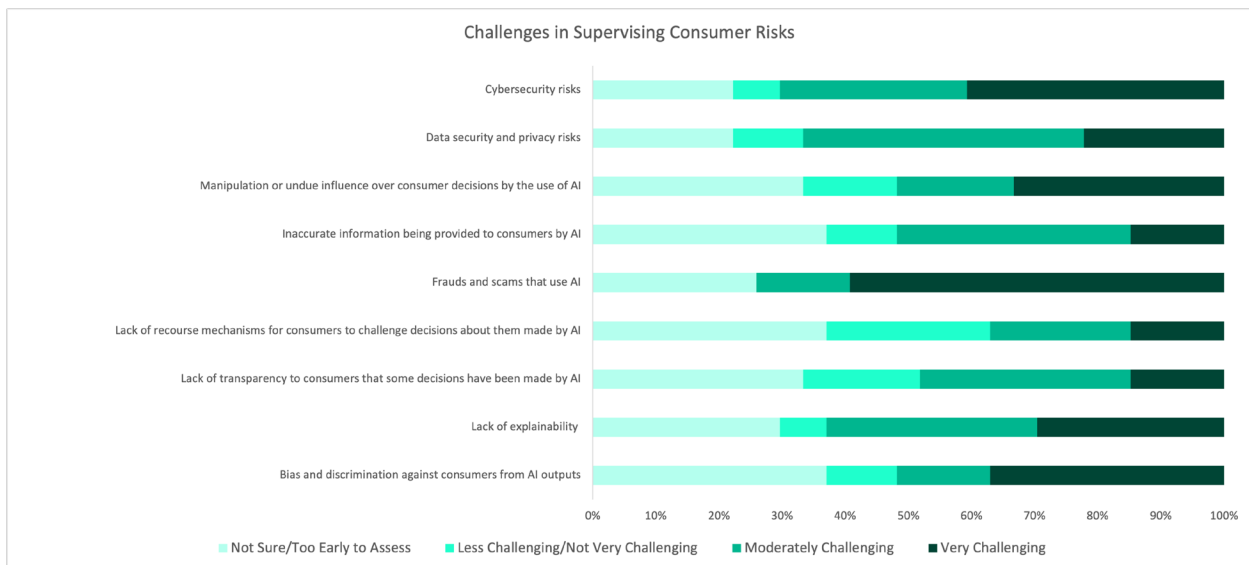
Source: World Bank Survey on AI in Supervision, 2025.

**Figure 4.2:** Consumer risks relating to frauds and scams using AI, cybersecurity, and data security and privacy currently seem to be of highest concern (n=27)



Question -“How would you rate the following risks to consumers in the next 5 years from the use of AI by financial institutions in your jurisdiction?”  
Source: World Bank Survey on AI in Supervision, 2025.

**Figure 4.3:** Supervision of consumer risks relating to fraud and scams is viewed as challenging by most authorities, but there also seems to be some significant supervisory uncertainty more generally (n=27)



Question -“How challenging is it to supervise the following consumer risks from the use of AI in financial services?”  
Source: World Bank Survey on AI in Supervision, 2025.

## 4.2 Supervisory responses to consumer risks

**Most authorities do not yet have a comprehensive understanding of AI adoption in their financial sector and its implications for financial consumer protection supervision.** This is understandable, given factors such as lack of information, competing priorities, and even difficulty in knowing where to start. EMDE authorities indicated in interviews varying degrees of readiness when it comes to understanding and addressing consumer risks emanating from the use of AI. The novelty of AI use cases in their financial sectors, even more so when it comes to GenAI use cases, and limited access to relevant skills and information are some of the reasons given for limited understanding of AI-related consumer risks. However, this is changing, and the recent rapid development in technology, as well as increasing AI uptake, is placing increasingly greater pressure on financial consumer protection supervisors to monitor and seek to mitigate potential risks.

**Ongoing industry engagement and data gathering on use cases is essential to inform authorities' responses to consumer risks from AI.** Most of the survey respondents that are actively taking steps to address consumer risks relating to AI have also been engaging in dialog with industry in this regard (Figure 4.4 and 4.5). Gaining a good understanding of how AI is being deployed by financial institutions in activities that affect consumers is key to informing effective supervisory and regulatory responses. This has been taking a variety of forms, including one-on-one engagements on specific AI deployments, discussions at industry fora, and thematic data-gathering exercises. For example, one EMDE authority has been engaging with financial institutions through a working group where industry participants share AI-related experiences.<sup>10</sup>

### Interviews with both EMDE and AE authorities

**suggest that engagement with AI-related consumer protection issues varies across jurisdictions and, in some cases, was limited even before the advent of GenAI.** Some authorities have undertaken more in-depth analysis of specific use cases, such as the use of chatbots or AI-driven product decisioning by supervised entities. Other authorities still appear to be taking a lighter-touch approach, even when it comes to more established AI uses such as those relating to credit assessments or insurance underwriting. The use of ML models for credit assessments has been growing for some time, with a range of already recognized potential consumer risks (see, for example, Langenbucher 2025 and FinRegLab 2023). However, based on some interviews, the level of scrutiny of such usage by authorities as part of their consumer risk assessments may vary significantly.

**The perceived lack of internal skills and knowledge by authorities when it comes to AI, referenced earlier, is of course also highly relevant to effective financial consumer protection supervision of AI-related risks.** Interviewed authorities mentioned various initiatives intended to assist supervisors in bridging knowledge gaps. They include the development of practical internal guidance to help supervisors better understand and engage with supervised entities on AI-related consumer risks and fostering ways to engage with the private sector on technology developments even beyond immediate supervisory activities. Other skills and knowledge building initiatives already discussed elsewhere in this report would also benefit FCP/market conduct supervision efforts in this area.

**A robust general consumer risk-assessment methodology, supported by a reasonably comprehensive general financial consumer**

10. For a discussion on industry engagement, not limited to AI issues, in the context of market monitoring see, for example, Consultative Group to Assist the Poor 2022.

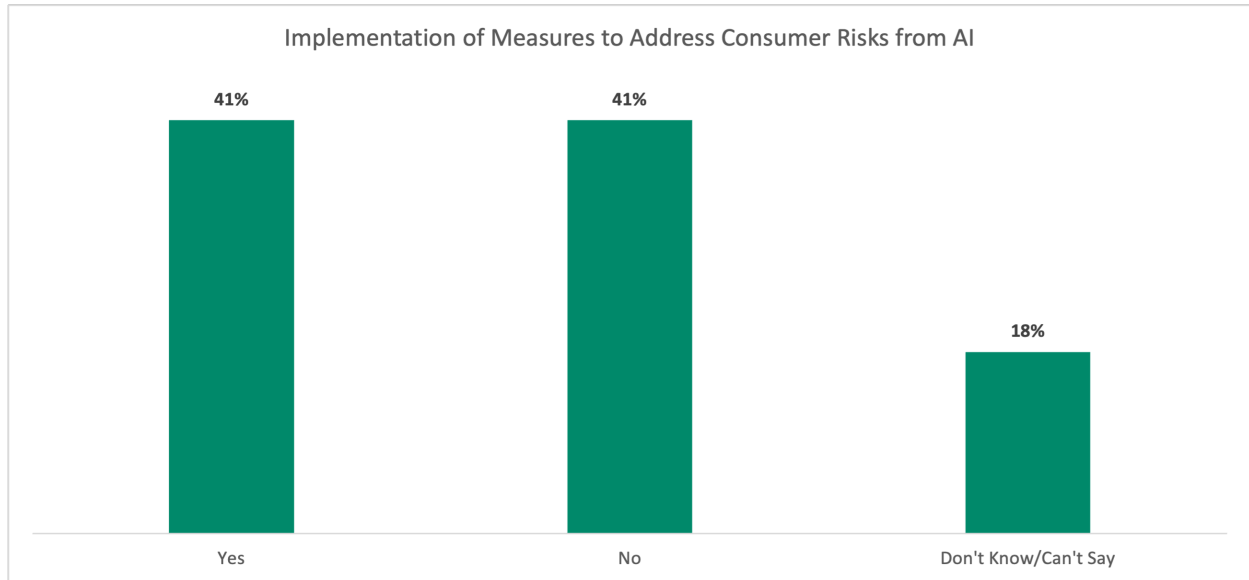
**protection regulatory framework, can be leveraged to address AI-related risks for consumers.** For example, one EMDE authority explained that they consider AI use cases as part of their broader financial consumer protection risk assessments and seek to understand potential risks to consumers in that broader context as well as controls implemented to address these. They do not necessarily plan to have any separate, dedicated AI-specific risk assessment approach. Another African authority similarly noted that their focus is on asking about, and understanding, internal measures that a financial institution has in place to address potential risks of their AI implementations. Consistent with this approach, for example, the International Association of Insurance Supervisors' (IAIS) recently released guidance on AI describes how key AI-related risks, including for consumers, should be supervised leveraging already established supervisory principles (IAIS 2025).

**Experiences of some developed EMDE authorities also suggest that risk assessments by supervisors will need to pay attention to a range of potential key gaps in financial institutions' management of key AI risks that remain unaddressed.** For example, the Australian Securities and Investments Commission's (ASIC) recent review of AI implementation by licensees found that while AI adoption is accelerating, many firms lack adequate frameworks and processes in comes to both assessing and managing consumer risks (see ASIC 2024).

**Most EMDE supervisory authorities are not necessarily moving to create new or revised AI-specific regulatory requirements when it comes**

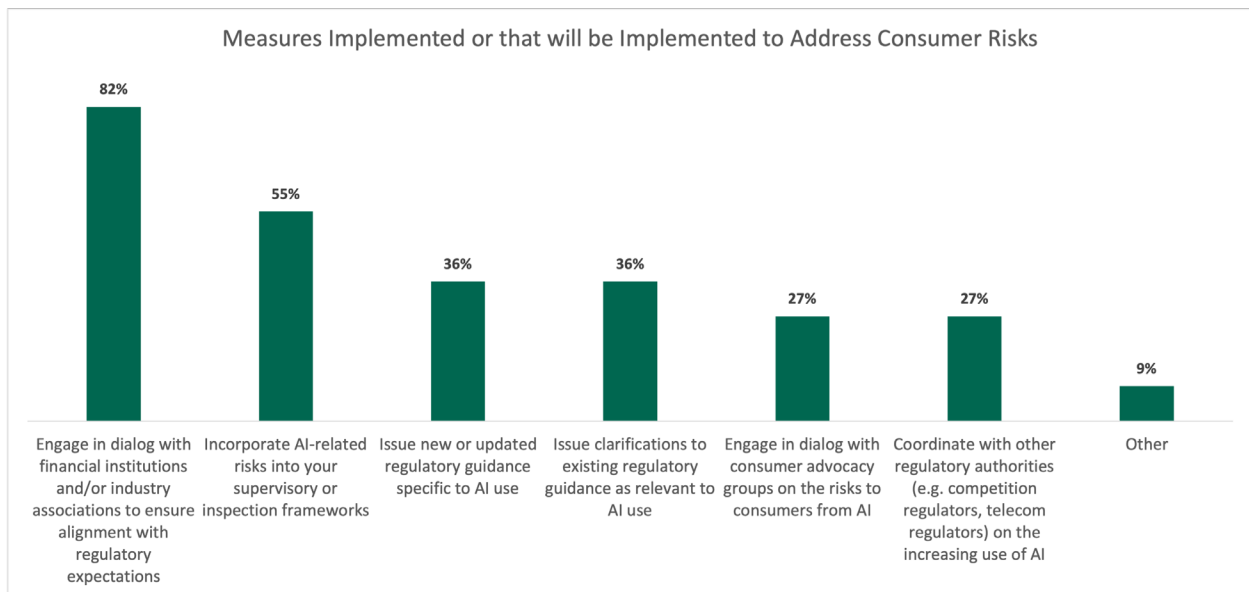
**to AI, at least not yet.** This is due to a range of factors, including that existing financial consumer protection obligations already apply to AI, even if they do not reference it specifically, and also that authorities are taking the approach of learning about relevant issues further before additional regulatory intervention (see, for example, Propson and Parker 2025). One authority interviewed for this report indicated that the existing regulatory framework in their jurisdiction already covers various issues relating to AI without needing to be specific about the technology. While some other specific provisions may be added in future, in other instances it may also be a matter of applying and interpreting existing regulatory requirements for AI uses. An African authority said that they were considering what, if any, disclosures they should mandate to make consumers aware that AI was used in decision-making processes, and how consumers may challenge such decisions. While the authority was aware of some financial institutions in their market making significant use of AI in processes such as product underwriting, which had generated some complaints, they had not yet determined how to best address this. Another EMDE authority was working on principles-based guidance for industry when it comes to AI-related issues, intended to both assist in fostering innovation and addressing risks. Nevertheless, it is also the case that some authorities are incorporating AI-related, or AI-relevant, provisions in digital financial services-specific reforms. (This may also raise a broader question to be considered regarding potential regulatory fragmentation and differential treatment of AI in different contexts, but this is beyond the scope of this report).

**Figure 4.4:** Most authorities are either not planning to implement, or cannot confirm, any specific measures to address AI consumer risks (n=27)



Question -“Has your authority implemented or plans to implement in the next 12 months specific measures to address consumer risks from the use of AI?”  
Source: World Bank Survey on AI in Supervision, 2025.

**Figure 4.5:** Authorities are implementing specific measures to address AI consumer risks (n=11)



Question -“Has your authority implemented or plans to implement in the next 12 months specific measures to address consumer risks from the use of AI? If yes, which measures? (select all that apply)”

Note: This figure is based on responses from the subset of responding authorities that indicated they have implemented or plan to implement specific measures to address consumer risks from the use of AI in the next 12 months.

Source: World Bank Survey on AI in Supervision, 2025.

# 5C

## COORDINATION AND COLLABORATION

**Oversight of AI in financial supervision increasingly depends on strong collaboration and coordination—both domestically and across borders.** Given the rapid evolution and complexity of AI technologies and the knowledge gap on AI adoption by the financial sector, collective efforts are needed to share knowledge and best practices and address emerging risks to enable responsible innovation and adoption of AI. Fragmented approaches risk regulatory blind

spots, inconsistent approaches, and duplicated efforts. By working together, including with private sector players, authorities can pool knowledge, align supervisory expectations, and respond more effectively to domestic and cross-border risks and market developments.



## 5.1 Between domestic authorities

---

**In several jurisdictions, AI expectations have been articulated at the national level and need to be interpreted and enforced by sectoral authorities with different mandates.** The plurality of mandates of relevant authorities (e.g., prudential, development, conduct, consumer protection, data-protection, and AML/CFT) gives rise to potential consistency and coordination challenges (also see Crisanto et al. 2024). The absence of a common AI definition and lexicon for the financial sector—or the uncertainty around its interpretation by different authorities—implies that new players and activities can slip through traditional regulatory perimeters, which can raise risks and stifle innovation.

## 5.2 Public-private engagement

---

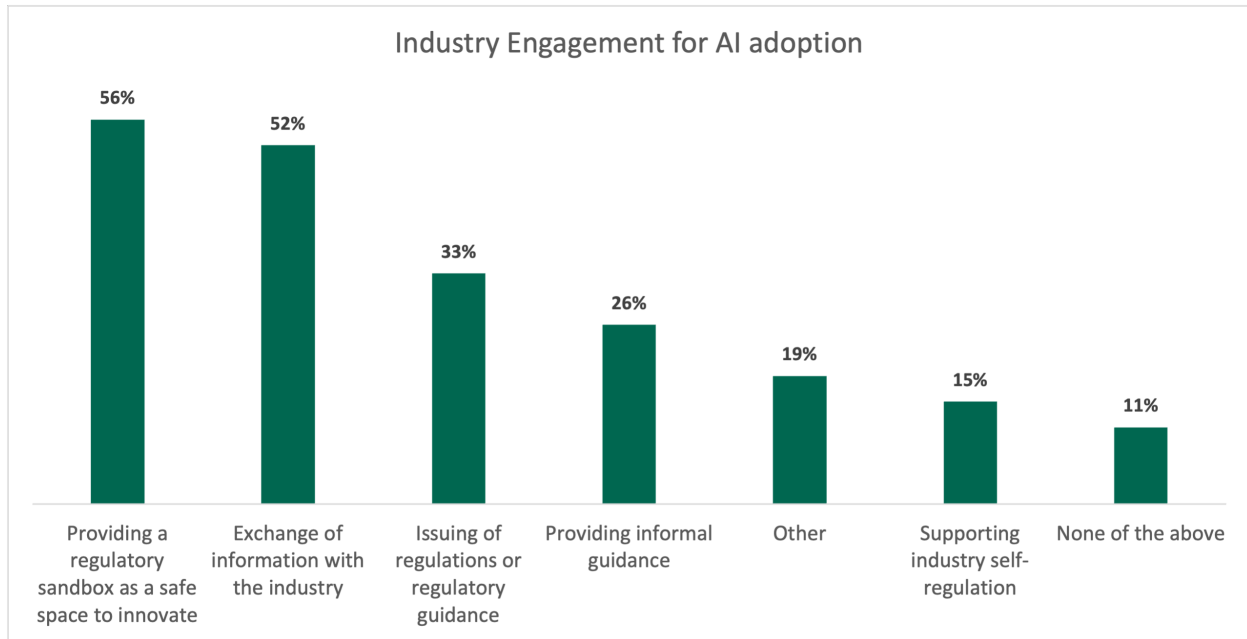
**Most financial authorities do not yet have a strong understanding of AI adoption by the financial sector and its implications for supervision.** Interaction with the industry is critical to understand, monitor, and respond to AI adoption and support responsible innovation by financial institutions, including fintechs. However, almost 50 percent of survey respondents do not have sufficient systems, resources, and processes in place to monitor and understand the use of AI in their financial sectors (Figure 2.4). As a result, financial sector authorities are not sufficiently aware of the main AI use cases in their markets and where there might be a need to intervene.

**As part of a multi-pronged strategy to bridge this knowledge gap, most jurisdictions are already engaging with the industry.** Survey respondents are mostly interacting with the industry through regulatory sandboxes (56 percent) and basic

**Financial sector authorities are aware of the need to work together with other domestic authorities to address gaps and overlaps as AI adoption challenges cut across sectors and mandates.**

There is a need for cross-sectoral cooperation by authorities to close information gaps, test whether current frameworks remain adequate, and address regulatory and supervisory gaps (also see FSB 2024). Various jurisdictions are addressing these issues through regular meetings that convene various authorities—typically via preexisting committees and groupings, but also de novo working groups—and joint publications, allowing for information exchange, the harmonization of institutional approaches, and an efficient allocation of resources.

information exchange (52 percent) (Figure 5.1). About one in three authorities are issuing or planning to issue AI-specific regulations or regulatory guidance to the industry, typically with the objective of encouraging responsible AI adoption while addressing risks such as data security, model risk, and customer protection. Several authorities also prepare periodic industry surveys and organize roundtables to improve their understanding of developments and gauge industry needs for regulatory clarity and guidance. Some survey respondents have set up thematic working groups with major banks and non-banks to discuss AI adoption in the industry, explore potential future AI use cases, and address concerns. One African authority is coordinating with the industry via various committees consisting of Chief Information Security Officers and Chief Compliance Officers of financial institutions.

**Figure 5.1:** Many jurisdictions are engaging with the industry (n=27)

Question -“In what ways is your authority engaging with the industry regarding the adoption of AI in financial institutions?”

Source: World Bank Survey on AI in Supervision, 2025.

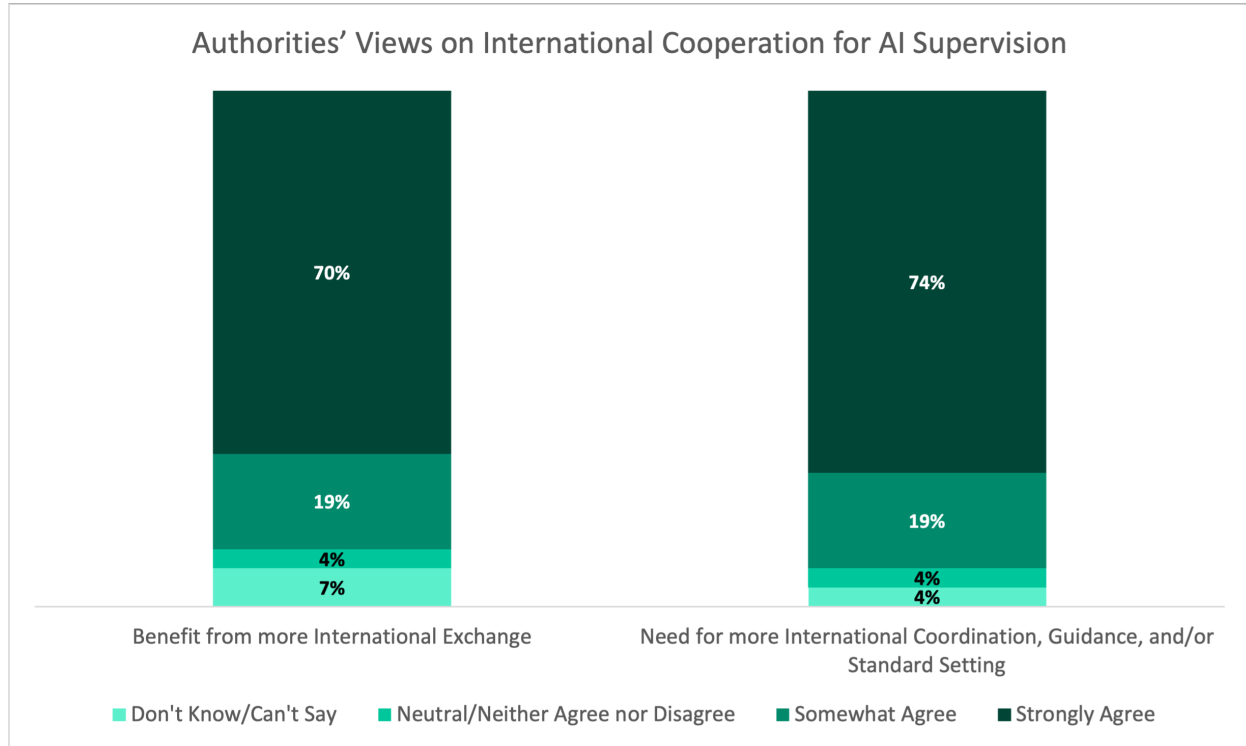
### 5.3 Across borders

**There is consensus among authorities that they would strongly benefit from cross-border information exchange.** Virtually all survey respondents recognize significant value in sharing best practices and industry developments across borders (Figure 5.2). Some authorities supervise banks that operate in several jurisdictions, prompting the need for bilateral collaboration (e.g., through existing structures such as supervisory colleges) and a harmonized approach across borders regarding AI (see Box 5). Several authorities are already exchanging information on AI through existing international bodies such as the Association of African Central Banks. Some African authorities mentioned that they have easy access to what their peers in the region are doing but gaining access to practices of financial sector

authorities outside Africa is challenging.

**Similarly, virtually all survey respondents signal a need for international guidance regarding AI.** Diverging AI definitions, taxonomies, and governance expectations risk fragmentation and regulatory arbitrage across countries (also see Crisanto et al. 2024). There is a role for international organizations to convene stakeholders; help assess data gaps; seek a shared understanding of AI use cases, risks, and supervisory responses; review policy adequacy and enhance supervisory capabilities and approaches; and coordinate on technology standards and oversight, particularly given the reliance of both financial sector authorities and the financial industry on cross-border service providers (also see FSB 2024, IAIS 2025 and IOSCO 2025).

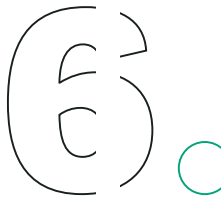
**Figure 5.2:** Jurisdictions see a strong need for international exchange of information and international guidance and standard setting regarding AI adoption for supervision (n=27)



Left chart Question - "My authority would benefit from more international exchange of information and best practices for supervision due to AI adoption in the financial sector." (Agree/ Disagree)  
 Right chart Question - "There is a need for more international coordination, guidance, and/or standard setting for supervision due to AI adoption in the financial sector." (Agree/ Disagree)  
 Source: World Bank Survey on AI in Supervision, 2025.

**Box 5: Cross border coordination**

The Committee of Central Bank Governors (CCBG), an association of 16 central banks within the South Africa Development Community (SADC), issued guidelines for the adoption of AI by its members. This framework provides central banks and financial sector supervisors with a structured approach to adopting AI responsibly. It covers governance, risk management, data discipline, and model oversight while embedding ethical safeguards and privacy controls. Key topics include AI strategy, lifecycle management, risk taxonomy, and collaboration mechanisms. The roadmap offers a blueprint for a phased implementation plan, starting with governance setup and pilots, enabling sustainable adoption and cross-border cooperation. It aims at aligning AI initiatives with supervisory mandates, strengthening readiness, and supporting capacity building for effective oversight.



## LOOKING AHEAD

**This report provides insights into the state of AI adoption in financial sector supervision in EMDEs, offering a foundation for several preliminary, forward-looking considerations for financial sector authorities.** While adoption of AI in EMDEs for financial supervision is at an early stage, most authorities aim to unlock AI's benefits while managing the associated challenges and risks. Experiences differ across countries but several preliminary considerations for EMDE authorities emerge from this report:

- **Take a strategic approach to AI adoption.** Authorities will benefit from a board-level governance framework to align their AI innovation and adoption with organizational

objectives and the need to maintain public trust. For example, implementing clear decision-making processes, accountability mechanisms, and a regular evaluation of AI tools and their impact on supervisory activities is important. Authorities should consider adopting a comprehensive approach to mapping supervisory processes to identify areas where AI can be most effective. Supervisors should retain final authority over AI-assisted supervisory decisions and be able to explain their rationale. And financial institutions must gain a thorough understanding of their AI applications and be accountable for model outputs and decisions.



- **Focus on foundational IT and data issues.** Authorities need to catch up in establishing integrated internal IT and data infrastructures necessary to support effective AI adoption, as well as effective SupTech adoption more generally. A key constraint is the lack of sufficient, high-quality digitized data for training and using AI models. Authorities have wide-ranging approaches to leveraging cloud services for AI with issues such as vendor dependency, data security, and data sovereignty emerging as common challenges.
- **Address skills and knowledge gaps.** Building internal knowledge and skills on AI-related matters is fundamental. Integrating both domain knowledge and new digital skills into supervision teams is crucial to identify supervisory use cases and implement them successfully. EMDE authorities need to develop systematic approaches to attract, retain and develop the right technical skills and expertise, as well as to keep supervisors up to date on technological developments relevant to their work.
- **Strengthen monitoring of AI developments in the industry, including risks.** Many authorities currently lack adequate systems, resources, and processes to monitor AI developments in the financial sector and should consider strengthening their capacity to monitor such developments and understand the associated opportunities and risks.
- **Foster coordination and collaboration.** Fragmented approaches to AI risk regulatory blind spots, inconsistencies, duplicated efforts, and the buildup of vulnerabilities. Authorities should foster collaboration and coordination with the industry, other domestic authorities, and across borders. Given the rapid evolution and adoption of AI, collective efforts to better monitor AI developments and assess impacts and exchange information and best practices are paramount.

# References

Allen, Hilary. 2023. "Regulatory Innovation and Permission to Fail: The Case of Suptech." *Journal of Law & Business* 19, no. 2. New York University.

ASIC (Australian Securities and Investments Commission). 2024. *Beware the Gap: Governance Arrangements in the Face of AI Innovation*.

Bank for International Settlements (BIS). 2025. *The use of artificial intelligence for policy purposes*.

Bank of England. 2023. *SS1/23 – Model risk management principles for banks (Supervisory statement 1/23 dated May 17, 2023)*.

Barrett, C. 2025. "Think You're Too Smart to Be Caught by Scammers? Think Again." *Financial Times*, 2025.

Bell, S., B. Gadanecz, L. Gambacorta, F. Perez-Cruz, and V. Shreeti. 2025. *Artificial Intelligence and Human Capital: Challenges for Central Banks*. BIS Bulletin No. 100. Bank for International Settlements.

Cambridge Suptech Lab. 2024. *State of Suptech Report 2024*. Cambridge: Cambridge Center for Alternative Finance.

Central Bank of the UAE. 2022. *Model Management Standards (Version date: November 2022)*.

Chettier, M. T., and V. A. K. Boyina. 2025. "AI-Powered Fraud Detection and Cybersecurity in Banking." In *The Impact of Artificial Intelligence on Finance: Transforming Financial Technologies*, edited by S. K. Gupta, J. Rosak-Szyrocka, R. Rena, C. S. Shieh, and G. Erkol Bayram, 53. Cham: Springer.

Consultative Group to Assist the Poor. 2022. *Market Monitoring for Financial Consumer Protection – Tool 6 – Industry Engagement*.

Consultative Group on Risk Management. 2025. *Governance of AI Adoption in Central Banks*. BIS Representative Office of the Americas, Bank for International Settlements.

Crisanto, J. C., C. B. Leuterio, J. Prenio, and J. Yong. 2024. *Regulating AI in the Financial Sector: Recent Developments and Main Challenges*. FSI Insights on Policy Implementation No. 63. Basel: Bank for International Settlements.

Dohotaru, Matej; Prisacaru, Marin; Shin, Ji Ho; Palta, Yasemin. 2025. *AI for Risk-Based Supervision: Another Nice to Have Tool or a Game-Changer*. Prosperity Insight Series. © World Bank.

European Commission: Directorate-General for Communications Networks, Content and Technology and Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji. 2019. *Ethics guidelines for trustworthy AI*, European Union Publications Office.

Financial Services Agency of Japan. 2021. *Principles for Model Risk Management* – November 12, 2021.

FSB (Financial Stability Board). 2025. *Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector*.

FSB (Financial Stability Board). 2024. *The Financial Stability Implications of Artificial Intelligence*.

FinRegLab. 2023. *Explainability & Fairness in Machine Learning for Credit Underwriting*.

Heikkila, M. 2024. “Artificial Intelligence Has Brought a Big Boost in Productivity—to the Criminal Underworld.” *MIT Technology Review*, 2024.

High-Level Committee on Programmes (HLCP). 2022. *Principles for the Ethical Use of Artificial Intelligence in the United Nations System*. United Nations System.

IFC (International Finance Corporation). 2024. *Governance and Implementation of Artificial Intelligence in Central Banks*. IFC Report No. 18. Washington, DC: International Finance Corporation.

IAIS (International Association of Insurance Supervisors). 2025. *Application Paper on the Supervision of Artificial Intelligence*.

IMF (International Monetary Fund). 2023. “Financial institutions are forecast to double their spending on AI by 2027.” December.

IOSCO (International Organization of Securities Commissions). 2025. *Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges*.

Langenbucher, K. 2025. "AI and Financial Services." In *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, edited by N. A. Smuha. Cambridge: Cambridge University Press.

Lopes, Ligia, Jennifer Chien, Mackenzie Wallace, and Edoardo Totolo. 2021. *The Next Wave of Suptech Innovation: Suptech Solutions for Market Conduct Supervision*. Washington, DC: World Bank.

National Institute of Standards and Technology. 2023. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, U.S. Department of Commerce.

Organisation for Economic Co-operation and Development (OECD). (2024), *Consumer Finance Risk Monitor*, OECD Publishing, Paris.

OECD. 2019. *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449. OECD Legal Instruments.

Perez-Cruz, F., and H. S. Shin. 2025. "Putting AI Agents Through Their Paces on General Tasks." *BIS Working Papers*, no. 1245, February. Basel: Bank for International Settlements.

Perez-Cruz, F., Prenio, J., Restoy, F. and Yong, F. 2025. "Managing explanations: how regulators can address AI explainability" *BIS Occasional Paper*, no. 24, September. Basel: Bank for International Settlements.

Prenio, J. 2025. "Starting with the basics: a stocktake of gen AI applications in supervision." *FSI Briefs* 26. Basel: Financial Stability Institute, Bank for International Settlements.

Prenio, J. 2024. "Peering Through the Hype – Assessing Suptech Tools' Transition from Experimentation to Supervision." *FSI Insights* 58. Basel: Financial Stability Institute, Bank for International Settlements.

Shabsigh, Ghiath, and El Bachir Boukherouaa. 2023. *Generative Artificial Intelligence in Finance: Risk Considerations*. Washington, DC: International Monetary Fund.

Propson, D., and D. Parker. 2025. *Artificial Intelligence in Financial Services*. AI Governance Alliance, World Economic Forum, in collaboration with Accenture.

Renier, J., L. White, H. Anderson, and J. Lao. 2025. "Combating Fraud and Scams in Fast Payment Systems." In *Institute of International Finance Digital Finance Developments*.

U.S. Department of the Treasury. 2024. *Artificial Intelligence in Financial Services: Report on the Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector*. Washington, DC: U.S. Department of the Treasury.

World Bank. Forthcoming. Finance and Prosperity 2025 flagship report.

World Bank. 2024. *Regulating Digital Data in Africa*. Governance and the Digital Economy in Africa Technical Background Paper Series. Washington, DC: World Bank.

World Bank. 2017. *Good Practices for Financial Consumer Protection: 2017 Edition*. Washington, DC: World Bank.

# ANNEX: SURVEY AND INTERVIEW PARTICIPANTS

## Financial sector authorities in African emerging markets and economies (EMDEs)

1. Banco de Mozambique
2. Bank Al-Maghrib
3. Bank of Ghana
4. Bank of Namibia
5. Bank of Tanzania
6. Banque des Etats de l'Afrique Centrale (BEAC) (Member states are Cameroon, Central African Republic, Chad, Equatorial Guinea, Gabon, and the Republic of the Congo)
7. Central Bank of Egypt
8. Central Bank of Kenya
9. Central Bank of Madagascar
10. Central Bank of Nigeria
11. Central Bank of Tunisia
12. La Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) (Member states are Benin, Burkina Faso, Côte d'Ivoire, Guinea-Bissau, Mali, Niger, Senegal and Togo)
13. National Bank of Ethiopia
14. Reserve Bank of Malawi
15. Reserve Bank of Zimbabwe
16. South African Financial Services Conduct Authority
17. South African Reserve Bank - Prudential Authority

## Financial sector authorities in other EMDEs

18. Banco Central do Brasil
19. Bangko Sentral ng Pilipinas
20. Bank Negara Malaysia
21. Bank of Thailand
22. Reserve Bank of India
23. State Bank of Pakistan
24. Superintendencia de Servicios Financieros del Banco Central del Uruguay
25. Türkiye - Banking Regulation and Supervision Agency
26. Superintendencia de Banca y Seguros del Perú (SBS)
27. Dubai Financial Services Authority (United Arab Emirates)

## Financial sector authorities in advanced economies

1. De Nederlandsche Bank
2. European Central Bank
3. Financial Supervisory Service Korea



**THE WORLD BANK**

IBRD • IDA | WORLD BANK GROUP

