August 12, 2024

Ms. Nellie Liang
Under Secretary for Domestic Finance
U.S. Department of the Treasury

Submitted via http://www.regulations.gov

INSTITUTE OF INTERNATIONAL FINANCE

Dear Madam,

Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector

The Institute of International Finance (**IIF**) welcomes the opportunity to publicly respond to the U.S. Treasury's (**UST's**) request for information (**RFI**) released June 6th, 2024.

We consider it very timely that the U.S. Government is seeking information on this important topic, both in view of the growth in potential applications for artificial intelligence (**AI**) in the financial sector and in view of the increasing official sector focus globally, across industries, that will require a steady hand and very thoughtful approach that takes into account risk management practices in the financial industry that are already in place, including for existing uses of AI. The IIF supports UST's commitment to fact-finding to better understand applications before considering the application of more advanced forms of AI, like generative AI (**GenAI**) and large language models (**LLMs**), that deserve deliberate thought.

We note the UST's role as a member of the White House AI Council established by President Biden's October 30, 2023 Executive Order on AI (**EO**). We recognize the desirability of the UST being well apprised of this topic in order to inform the deliberations of that Council, particularly insofar as they are relevant to the financial sector and particularly as the Council coordinates the potential development of horizontal or cross-sectoral AI-related policies that could impact the financial sector even if not targeted specifically to the financial sector.

The IIF represents approximately 400 globally active financial institutions from over 60 geographies, drawing from the banking, insurance, securities, asset management, payments and other sectors. Many of our members are particularly interested in cross-border impacts of emerging technologies and related regulatory frameworks. While this RFI focuses on AI, the IIF would highlight new cross-border work currently being pursued on issues around data access and data free flow with trust, to which the UST is also a party, and the importance of that work to the RFI being addressed here.

Factual background

The IIF and its members have been very focused on AI in finance for some years, most notably through the IIF's periodic surveys of its members on this topic. This important survey and data series has been carried out since 2018 and, since 2022, in partnership with EY. In December, we published the 2023 IIF-EY Public Survey Report on AI / machine learning (**ML**) use in financial services (**2023 survey report**). We draw on this data series, which we are currently in the process of extending with the issuance of the 2024 survey this past May, in answer to many of the questions in the RFI in **Annex I**. The IIF also maintains an AI/ML Experts Group comprised of senior business representatives across its global membership, with profiles including firms' global heads of AI or model risk management, that meets quarterly.

Drawing on recent discussions with this Experts Group, and frequent bilateral contacts with our members, we observe the following:

- The role of AI in financial services is transitioning from conceptual excitement to practical implementation in 2024. At this time, financial institutions are primarily focusing on operationalizing AI models that draw on their own data, using processes they are mostly familiar and comfortable with, now moving beyond just risk-focused applications to explore value-creating use cases. They are looking for opportunities to benefit the financial industry as a whole by aligning applications with clear strategic priorities. Financial firms are primarily testing these

models internally, with the desire to better understand and employ AI in a manner that is safe for consumers, and many of them are proactively engaging their regulators as they proceed.

- Key areas for AI application in finance include efficiency gains (e.g., coding assistance, report generation), improved customer experiences (e.g., personalized service, micro-marketing), and enhanced decision-making (e.g., pricing, fraud detection, and AML). GenAI shows particular potential for improving unstructured data utilization, which could have a significant positive impact on the industry.
- Scaling projects to production is a current challenge. Financial institutions are prioritizing core capabilities and infrastructure upgrades in data, cloud, and APIs that are equally or more important than new investments in advanced AI applications. Balancing control and market speed is crucial and top of mind already for financial services firms, with solutions emerging in pre-deployment (e.g. integration of model risk management teams early in the product development process) and post-deployment phases (e.g. automatic risk assessment, machine-readable controls).
- The advent of GenAI has led financial entities to review some existing governance practices for AI in finance, considering the step-change in capability of the technology. Most GenAI tools are provided by third parties, creating complex relationships and visibility issues for financial institutions in model validation and risk management, including for privacy and confidentiality. Financial services firms are still working through these complexities, again explaining the primary focus being on internal-facing and lower-risk employment of models, to date.
- Financial services firms have various frameworks already in place to ensure they operate sensibly and safely with respect to the exploration and adoption of any new technology. These general operating practices of a firm, and the existing regulatory framework in the financial industry, reflect more conservative behavior by the financial industry than general public discussion on AI might suggest. [1]
- Cloud infrastructure is critical for AI development and deployment, particularly for GenAI. It provides necessary computational power and data resources, enabling both large and small firms to leverage AI technologies. The AI supply chain is complex but distributed, involving various providers and technologies across the hardware and software landscapes.
- The regulation of AI affecting financial services is evolving, with different jurisdictions and different industry regulatory agencies taking varied approaches. In jurisdictions that have quickly forged ahead with comprehensive AI regulation, such as the EU, IIF members observe that in some cases AI applications that have been safely employed for years are getting swept up in an over-reaching umbrella of new regulation. They also observe unclear liability rules that have resulted from such regulations, and potentially conflicting sector-specific and general AI regulations. This is in contrast to jurisdictions that have, to date, taken a principles-based approach to this general-purpose technology.
- The financial services industry, with its experience in handling sensitive data and cloud technology, is well-positioned to inform policy development for AI transparency and trust-building. It also has much practice already with the employment of traditional uses of AI, which the U.S. Government and official sectors globally might draw on to better inform their approach to other industries that are less developed in their approach.

A summary of the 2023 survey report is contained in **Annex II**. Some of the top-level findings of the 2023 survey are:

- AI/ML usage in financial institutions is widespread and growing rapidly, with 84% of surveyed firms using AI/ML in production. The number of use cases is expected to increase significantly, especially in risk and compliance, operations, technology, and retail/consumer areas.
- GenAI is seen as a step-change in AI technology, with 86% of respondents anticipating expansion in their model inventories. Near-term use cases include risk assessment, code assistance, document querying, and financial crime prevention. Most institutions plan to use GenAI primarily for internal, non-customer-facing deployments initially.

[1] For example, internal AI policies often set out governance and oversight rules, including model risk management policies that also apply to AI and GenAI models (e.g. U.S. SR 11-7 or OSFI E-23 Guidelines).

- Benefits of AI/ML in finance include discovering new risk patterns, cost savings, increased model accuracy, and improved efficiency in processes like credit risk management, pricing, and anti-money laundering efforts.
- Governance and regulatory engagement are key focus areas, with 66% of respondents having or planning to have a C-suite officer responsible for AI/ML ethics. Explainability and bias are top issues in discussions with regulators, and many firms are developing new frameworks specifically for AI/ML governance.
- Regarding governance structures for AI/ML, 41% of respondents are extending existing model risk management or enterprise risk management frameworks, while 39% are building or have built new, complementary frameworks.
- This indicates growth towards specialized governance for more advanced, emerging AI technologies, while importantly drawing on frameworks that firms already have well in place for more traditional uses of AI.

Key considerations for the official sector

Against this factual background, we suggest that UST and U.S. regulators bear in mind the following key considerations as they consider responses to the RFI:

- **AI is not new:** While GenAI at scale is a relatively emerging technology, the official sector should avoid adding to or exacerbating hyperbole around AI. AI and ML have long histories in the financial services industry and are already subject to existing risk frameworks (see below). Many sophisticated analytical systems and ML engines have been successfully in operation for years, including in credit risk scoring, high-frequency trading, and robo-advice.
- **AI in finance is already regulated:** AI applications in finance are already subject to regulation through sectoral or cross-sectoral regulations. Examples include client confidentiality rules, consumer data privacy regulations, market regulator rules on robo-advice or high-frequency trading, consumer protection regulation in lending operations, or prudential requirements concerning data governance, cyber risk, third-party risk, information systems outsourcing, or operational risk generally. All of these regulations apply to the use of any general-purpose technology, like AI, in financial services, ensuring that material risks are well managed. The financial industry is already more heavily regulated than others.
- **Existing risk frameworks are foundational:** Financial institutions (whether banks, insurers, securities firms, infrastructures or others) operate under prudential requirements that require FIs to develop their own sophisticated risk management governance frameworks, systems, and controls. These arrangements have largely served the industry well, including those directed at disaster recovery and business continuity. FIs keep such arrangements under constant review and make adjustments as needed, proactively. The industry starts from a very strong risk management foundation – one that is commensurate with and contributes to the high trust placed in financial institutions by their clients.
- **Immediate regulation not warranted:** At this stage, we do not believe that technology-specific regulation in the U.S. with respect to AI as a broad category, or within just the financial services industry, is warranted or desirable. We believe supervisory measures, including fact-finding and research, to be the right approach in the short- to medium-term while other industries catch up to the financial industry's level of understanding and experts evaluate potential benefits and risks more thoroughly. There is a lot still to be understood.
- **AI and data** are inexorably interlinked; understanding these connections and their implications for each participant in the value chain is important to appropriately reflect business realities. AI requires access to sufficient volumes of quality data; restrictions to data sharing limit its potential and even risk creating bias and other distortions. These issues can lead to overfitting, where models perform well on training data but poorly on new data, and underfitting, where models fail to capture meaningful relationships between inputs and outputs, further impacting model accuracy. Data localization requirements may contribute to this risk.

For reference, it is worth noting that our discussions with official sector senior staff indicate that various global financial standard-setters believe AI is not sufficiently understood to pursue global standards anytime soon. The IIF recently discussed FIs' use of AI during a two-hour special session hosted by the

Financial Stability Institute at the 2024 BIS Annual General Meeting on a panel that included the Secretary Generals of IOSCO, IAIS, and BCBS. This recorded session can be viewed here and provides direct insight into the views of these global authorities on this issue. At a jurisdictional level, the IIF does see some potential for a patchwork of approaches forming, that could impact competitiveness generally.

Further engagement

The IIF and its members stand ready to engage in additional discussions and consultations on these topics, or to clarify any aspect of our submission.

For example, if desired we could convene a meeting of interested IIF members with Treasury officials to discuss the RFI and this submission further.

A restricted version of the 2023 IIF-EY survey on AI/ML Use in Financial Services, which contains a more robust dataset than in the Public Survey Report, is accessible to survey respondents and policymakers. We are happy to brief Treasury officials on the more granular findings of the survey or share the restricted version with the Treasury if the non-public nature of the fuller dataset can be maintained.

We thank you again for the opportunity to contribute to this important consultation.

Yours sincerely,

Jessica Renier
Managing Director, Digital Finance

Annex I

Answers to RFI questions

Unless otherwise stated, data points from the 2023 survey report are as at the survey date, i.e. June-August 2023. Other results are as at the survey dates in the respective reports.

The 2023 survey included a globally diverse group of 65 financial institutions, drawn from the IIF's membership, from across nine regions, responding to questions on AI/ML usage, governance and controls in financial institutions. Survey respondents included banks (G-SIBs, internationally active banks, national banks), insurers, and others (e.g., Central Bank, Brokerage, Asset Manager, Clearinghouse, Multilateral Organization).

We note that the RFI specifically allows for partial answers. Questions in the RFI that are treated as subsidiary questions to which a separate answer is not provided are not reproduced in this Annex.

Question 1: Is the definition of AI used in this RFI[2] appropriate for financial institutions?

The definition emphasizes AI's role in making "predictions, recommendations or decisions influencing real or virtual environments." We acknowledge the definition reflects the OECD Council's definition of AI System, although we note that that definition included "content" as a fourth output type. AI in the financial sector can also be used for security purposes minimizing operational risks, by automating manual procedures. We acknowledge also that this is the definition of AI in President Biden's October 30, 2023 Executive Order on AI (**EO**).

We suggest that this definition may be too broad as it risks capturing a broad range of ordinary technology, and could capture advanced statistical techniques or other programmed techniques that have neither adaptivity nor autonomy as required by the definitions of AI in the EU AI Act (Art. 3(1)) and similarly in the previous U.K. Government's White Paper on AI (at 3.2.1), and may be too broad for many analytical or regulatory purposes.[3]

We would also wish to emphasize that the boundary of what is considered AI for analytical purposes is not necessarily appropriate for defining the subject-matter of any technology-specific regulation. As stated, for the reasons stated in the cover letter, at this stage, we do not believe that technology-specific regulation, particularly any targeted at the financial industry alone, in the U.S. of AI as a broad category is warranted or desirable in the short-term.[4]

Moreover, if regulators keep to a technology-neutral approach and focus on outcomes and activities rather than specific technologies, a definition would be unnecessary.

Question 2: What types of AI models and tools are financial institutions using? To what extent and how do financial institutions expect to use AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing?

---

[2] The RFI adopts the definition of AI utilized in the EO, i.e. 'The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human – based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.' (RFI, p. 8)

[3] Our own working definition of AI for the purpose purely of our survey work differs from that used in the RFI and draws on existing work of the Financial Stability Board (FSB): "The theory and development of computer systems able to perform tasks that traditionally have required human intelligence. It is broadly applied when a machine mimics cognitive functions that humans associate with other human minds, such as learning and problem-solving." The emphasis on mimicking human intelligence in this definition would seem to exclude advanced statistical techniques or other programmed techniques that have neither adaptivity nor autonomy. 2023 survey report, Glossary, p. 23.

[4] (We note in any case that the FSB has announced it will review its 2017 paper on financial stability implications of artificial intelligence.)

Types of AI models and tools: The 2023 survey report defined ML as one of the techniques used for AI and includes neural networks, among others. Example AI and ML approaches within the scope of the survey include:

- Ensemble methods (e.g., gradient boosting machine, random forest, and isolation forest)
- Neural networks (trained through supervised, unsupervised, or semi-supervised learning)
- Kernel or instance-based algorithms (e.g., support vector machines and support vector regression)
- Complex dependence structure (e.g., hidden Markov models, Bayesian networks, and generative adversarial networks)
- Online or reinforcement learning (e.g., Q-learning, state-action-reward-state-action and adaptive dynamic programming)
- Natural language processing (**NLP**)
- Speech recognition and generation
- Image recognition, classification and generation.

While NLP is an important AI/ML technique, only 16% of respondent financial institutions in the 2023 survey claim to have 50 or more natural language processing use cases in their model inventory.

In our 2022 survey, it was reported that the majority of financial institutions surveyed apply machine learning techniques in production for credit risk management, and the adoption of ML usage in production for AML was at a similar level.[5]

Use cases: As at 2023, over the following three years, risk and compliance, operations, technology and data, and retail/consumer are predicted to be the most relevant areas of AI/ML usage for institutions surveyed. For the 2023 survey, a plurality of firms ranked marketing and operations as the functions with the most AI/ML use cases. Risk, compliance, fraud, and retail/consumer are functions that were also ranked as having AI/ML use cases by a broad set of respondents. As at 2023, retail/consumer credit risk, compliance risk, and operational risk were ranked as the risk stripes with the most AI/ML use cases. In addition to the response options, survey respondents identified fraud risk, operational efficiencies, internal validation and controls, ESG, reputational risk, and conduct risk as specified AI/ML use cases.[6] Models employed in the collections space can also be powered by AI.

As to GenAI use cases, see our response to Question 3.

Level of deployment in production: As at 2023, 84% of respondent institutions are applying AI/ML techniques in production, and an additional 11% of respondents are either applying AI/ML techniques in pilot projects or planning on applying AI/ML techniques in the foreseeable future. All G-SIB respondents are currently applying AI/ML techniques in production. Moreover, the numbers of use cases in inventory is large and growing, with only a narrow majority (52%) of respondent institutions having fewer than 50 AI/ML use cases in their current model inventory; 19% having 50-150 AI/ML use cases; 11% having 150-250 AI/ML use cases; 3% having 250-350 AI/ML use cases; and a full 15% having more than 350 AI/ML use cases in their current model inventory.

Platforms/Infrastructure: As at 2023, 59% of respondent institutions are currently using AI/ML model development and deployment platforms or infrastructure. An additional 31% of respondents are either experimenting with pilot projects or are planning on using AI/ML model development and deployment platforms or infrastructure in the future. When viewed by institution-type, a broad majority of G-SIBs and insurers are using such platforms in production, and a majority of international banks and national banks are as well.[7]

---

[5] IIF-EY (December 2022), Survey Report on Machine Learning — Uses in Credit Risk and Anti-Money Laundering Applications.
[6] This paragraph is based on the participants' and regulators' version of the survey report. See covering letter.
[7] 2023 survey report, p. 13.

Question 3: To what extent does the type of AI, the development of AI, or AI applied use cases differ within a financial institution? Are there any related reputation risk concerns about using AI?

Use cases: The 2023 survey report contained a separate chapter on GenAI. As at 2023, in the near term (next 12 months), 81% of respondents expect GenAI to be used primarily for internal deployments (non-customer facing), including 100% of U.S. institutions. Examples of near-term use cases include risk identification and assessment, code assistance, document querying and extraction, and financial crime/AML. Over the next three years from mid-2023, respondents expect an increased focus on external use cases and the use of GenAI in ecosystems (integration across functions and third parties).

Reputation risk: 77% of respondents to the 2023 survey report impose at least some restrictions on the use of GenAI or fully ban its use, and 40% nominated reputational risk as a risk in respect of which the organization had policies/procedures to control the risk due to the use of GenAI. While GenAI offers significant advancements as just mentioned (risk identification and assessment, code assistance, document querying and extraction, to name a few), it also raises ethical, privacy and employment concerns that may suggest the need for complementary controls, including when interacting directly with consumers.

Question 4: Are there challenges or barriers to access for small financial institutions seeking to use AI?

While the IIF's survey reports on AI/ML use don't isolate challenges or barriers to access faced by small financial institutions, some of the challenges studied could be more pronounced for smaller entities. For example, in the 2023 survey, participants selected as the primary challenges for launching AI/ML tools in production: data quality, supervisory understanding or consent to use new processes, staff skillsets, underlying technology infrastructure, and explainability.[8] Some of these, particularly staff skillsets and underlying technology infrastructure, could be more significant barriers for smaller institutions with limited resources. Similarly, in the 2022 survey, IT infrastructure is mentioned as a challenge both for credit risk management and AML use cases, which could be a more significant issue for smaller institutions with limited resources for upgrades.[9] As another example, implementing robust data governance could be more challenging for smaller institutions to implement comprehensively.

A primary barrier to uptake and deployment at scale of AI in the financial sector is the interrelated issues of data quality and availability. While financial institutions control high-quality structured datasets, typically comprising information submitted when a customer applies for a new product such as a loan or insurance policy, they may lack real-time information and social graph data available to other players including non-bank PSPs and social media platforms. This limitation is exacerbated by the absence in most geographies of a robust, horizontal data access framework that would enable financial institutions, regardless of their size, to access both financial and non-financial data relevant to enhancing their financial services offerings. Such a framework is essential for leveling the playing field and fostering innovation across the financial sector.

One factor to consider is that access to pre-trained LLMs could lower barriers to entry for smaller financial institutions. This is different from traditional AI, especially for supervised training; the size of the training data set is a key factor, such that larger financial institutions have a natural data advantage.

Question 5: What are the actual and expected benefits from the use of AI to any of the following stakeholders: financial institutions, financial regulators, consumers, researchers, advocacy groups, or others? How has the use of AI provided specific benefits to low-to-moderate income consumers and/or underserved individuals and communities? How has AI been used in financial services to improve fair lending and consumer protection, including substantiating information?

[8] p. 15
[9] IIF – EY (December 2022), *op. cit.*

Benefits: Participants in the 2023 survey report identified improved outcomes of using AI/ML techniques in financial institution processes. In descending order, they were (out of 65 responses):

1. Discovery of new risk segments and patterns (n = 50)
2. Cost savings
3. Increased model accuracy
4. Ability to conduct holistic analysis of different data sources
5. More efficiency in the model development process (increased speed, leaner processes)
6. Overcoming data deficiencies or inconsistencies (n = 26)[10]

The distribution of responses was relatively consistent across regions and institution types. Regarding usage, a European G-SIB using AI/ML in production noted that it utilizes AI/ML "mainly for business development and improving customer experience use cases."[11]

These results chime with results from earlier surveys in the series: for credit risk management, increased model accuracy was overall the most improved outcome observed when using ML techniques globally in our 2022 survey on this topic. Discovery of new risk segments/patterns and the ability to conduct a holistic analysis of different data sources were commonly improved outcomes as well.[12] For AML, institutions highlighted two key benefits: improving the efficiency of their models and discovering new risk segments/patterns. Furthermore, firms realized a reduction in false-positives through the use of machine learning and, in turn, a reduction in operating costs.[13]

Customer experience has also improved by the use of AI in biometric authentication for example by face recognition with neural networks or voice proof of life with natural language processing. This technology can lead to an increase in financial inclusion while also increasing the safety and security of financial services, while also being vulnerable to advances in deepfakes. AI is of course also at the forefront of the battle to detect deepfakes.[14]

Specific benefits to low-to-moderate income consumers and/or underserved individuals and communities; improved fair lending and consumer protection: In general, from an operational point of view, AI/ML allows for potentially large-scale, low-cost applications and democratizes access to high quality services for clients that may have been unprofitable to service under traditional workflows. The IIF-EY survey series contain a number of relevant data points. The adoption of AI/ML techniques has delivered tangible benefits to FIs, including improved model accuracy, the ability to overcome data deficiencies and inconsistencies, and discovery of new risk segments or patterns.[15] This could benefit underserved communities by making credit more accessible to creditworthy consumers who lack a formal financial record, and reduction of cross-subsidies between uncreditworthy and creditworthy account-holders. AI/ML could also help protect vulnerable consumers from financial difficulties. For example, AI/ML was used by one Canadian bank to identify which credit card customers were likely to pay late, and the bank was able to engage these customers proactively to help. This resulted in a reported reduction of arrears by 10%.[16] More automated use of credit scoring systems has been found to "reduce the possibility of unlawful discrimination by helping ensure consistency and uniformity and minimizing individual judgment and discretion."[17] Another more recent study analyzed the effects of the use of ML in mortgage lending in the U.S. The authors concluded that when deciding whether borrowers are granted mortgages, machine learning benefits disadvantaged groups. [18] The IIF in May 2019 reported that ML was used to correct biases against minorities and

---

[10] p. 15. Anecdotal evidence illustrating these expected benefits is cited at p. 14 of the 2023 survey report.
[11] p. 13
[12] IIF – EY (December 2022), *op. cit.*
[13] Ibid.
[14] IIF (2024), Takeaways from the Global Payments Forum.
[15] IIF (2019), Machine Learning Recommendations for Policymakers, p. 5.
[16] Daniel Moore, "Machine Learning in Risk Management", December 5th, 2018, cited in IIF (2019), *Machine Learning Recommendations for Policymakers*, p. 3.
[17] FDIC Supervisory Insights, "Fair Lending Implications of Credit Scoring Systems" (Summer 2005), cited in IIF (May 2019), Machine Learning Thematic Series Part II: Bias and Ethical Implications.
[18] Fuster, A, P Goldsmith-Pinkham, T Ramadorai and A Walther (2018), "Predictably Unequal? The Effect of Machine Learning on Credit Markets," cited in IIF (May 2019), *op. cit.*

women, placing "a high emphasis on the detection of outliers and on missing value imputation." For example, ML can help to overcome data gaps related to maternity leave, potentially leading to fairer credit decisions for women.[19]

Question 6: To what extent are the AI models and tools used by financial institutions developed in-house, by third-parties, or based on open-source code?

The 2023 survey report discusses third-party AI/ML usage in Section VII. A majority of respondent institutions expect the use of third-party AI/ML models to increase by 10-25% over the following 12 months from mid-2023[20], with around another sixth of respondents expecting an increase of between 25 – 50% and around another tenth of respondents more than 50%; fewer than a sixth of respondents expect no increase. The report doesn't provide specific percentages for in-house vs. third-party vs. open-source development.

Question 7: How do financial institutions expect to apply risk management or other frameworks and guidance to the use of AI, and in particular, emerging AI technologies? What types of testing methods are financial institutions utilizing in connection with the development and deployment of AI models and tools? To what extent are financial institutions evaluating and addressing potential gaps in human capital to ensure that staff can effectively manage the development and validation practices of AI models and tools? What challenges exist for addressing risks related to AI explainability?

Risk management: As stated in the cover letter, financial firms already have comprehensive existing risk management frameworks in place including operational risk, data governance and third-party risk. Like any form of technology a firm uses, AI is subject to these existing frameworks.

Section IV.A of the 2023 survey report discusses governance and oversight for AI/ML. Key points include that 66% of respondents have a C-suite officer of AI/ML governance currently or are in the process of designating one; 64% of respondents have an executive committee focused on AI/ML governance or are in the process of defining or aligning one; and 54% of respondents use a tollgate process for making decisions about proceeding with AI/ML use cases, and an additional 21% plan to introduce one. 78% of respondents have or are in the process of establishing policies or procedures to mitigate some of the risks posed by GenAI. Further details are provided in Section III.C of the 2023 survey report.[21]

Testing: Based on the results of our survey work, financial institutions are using a variety of testing methods for AI/ML models, focusing on performance, accuracy, explainability, and robustness. Model validation is heavily relied upon as a control for AI/ML risks. In order of importance, the following model validation techniques were all selected by at least 30 respondents, indicating a broad set of AI/ML model validation techniques are utilized by institutions:

- Ongoing performance monitoring
- Data quality validation
- In-sample/out-of-sample testing
- Outcome monitoring against a benchmark
- Validation of feature engineering process
- Implementation testing
- Explainability tools
- Outcome monitoring against a non-AI/ML model / A-B testing
- Benchmarking

[19] IIF (May 2019), *op. cit.,* p. 15.
[20] This includes 50% of the G-SIBs, a plurality of insurers, and a majority of international banks, national banks, and other institution types.
[21] Besides model risk management risks under management through such structures include: compliance/legal risks, third-party risks; cyber risks; technology risks; ESG risks, etc.

For GenAI specifically, respondents highlighted testing for hallucination, sensitivity analysis, benchmarking, toxic content, and boundary testing as key tests for validation.[22]

Gaps in human capital: The 2023 report highlights "availability of talent with the right set of skills" as a key challenge (p.15). 63% of respondents have implemented training or guidelines on AI/ML practices for employees (2023 report, p.12).

AI explainability: As with any other technology generated output, firms have processes in place for validating outputs of AI/ML systems to ensure accuracy and that the quality and substance of the output is fit for purpose.

Explainability is all the same consistently mentioned as a top challenge across our AI/ML survey reports. In the 2023 survey report, we reported that the top two issues raised by regulators/supervisors are explainability / "black box" nature of some algorithms and bias/ethical issues related to the use of AI/ML. These trends were consistent across institution types and regions. The use of explainability tools is reported as a technique in model validation by over 30 respondents.

An American G-SIB noted that, "global as well as local explainability is required as part of model development and review process where such risk is significant based on the model usage. [An] explainability center of excellence conducts research and evaluates new tools and methods" (p. 17). Global vs local interpretability was discussed in IIF (November 2019), *Explainability in predictive modelling*, section 3.1.3.

We also would highlight that:

- explainability is not a challenge for all AI/ML algorithms (e.g., the outcome of a logistic regression is fully explainable);
- depending on the use case, financial institutions decide on the best algorithms to use considering features such as explainability or accuracy. For certain use cases, explainability is not a requirement (e.g. in the case of a chatbot). In other cases, explainability is needed (e.g. when using AI outcomes in relevant decision-making processes, and institutions might decide to lose some accuracy gain to use more explainable algorithms); and
- the most complex algorithms are not always the ones that give the best results.

Question 8: What types of input data are financial institutions using for development of AI models and tools, particularly models and tools relying on emerging AI technologies? Please describe the data governance structure financial institutions expect to apply in confirming the quality and integrity of data. Are financial institutions using "non-traditional" forms of data?

Types of input data: Reports earlier in the survey series suggest that financial institutions are using both existing high-quality, structured credit or financial data sets sourced both from internal client data and from third parties, and unstructured data sets (such as news feeds, annual reports, network analysis of supply chains, or social media-sourced information) as inputs to AI/ML models including those that make use of NLP in the analytic pipeline.[23] Other data used to build AI models developed by third parties, includes soft data, for example related to mobile carriers, including monthly bills.

Data governance structure: The 2023 survey report mentions that 66% of respondents have a C-suite officer overseeing AI/ML governance currently or are in the process of designating one (p.11). 64% of respondents have an executive committee focused on AI/ML governance or are in the process of defining or aligning one (p.1). 54% of the respondents use a tollgate process, and an additional 21% plan to introduce one, for proceed/don't proceed decisions in AI/ML use cases (p.11). We would also remind that regarding governance structures for AI/ML, as of the 2023 survey, 41% of respondents are

[22] Exhibit 5.5 and accompanying text.
[23] See Machine Learning in Credit Risk (March 2018), p. 24, and Machine Learning in Credit Risk, 2nd edition: Summary Report (September 2019).

extending existing model risk management or enterprise risk management frameworks, while 39% are building or have built new, complementary frameworks.

Non-traditional / alternative data sources: The non-traditional or alternative forms of data mentioned in the survey series include news feeds, annual reports, supply chain information, social media-sourced information, and unstructured data sources. The reports also mention the use of transaction-level data and behavioral data in some contexts.[24] Institutions have also consistently expressed that access to more data sets could provide better results in the use of AI/ML technologies.

Question 9: How are financial institutions evaluating and addressing any increase in risks and harms to impacted entities in using emerging AI technologies?

Financial institutions are using auditing, testing, and controls as primary methods to mitigate against biased or discriminatory outcomes (2023 survey report, p.15-16). Some institutions are applying codes of ethics, both institution-wide and specific to AI/ML (*id.*). Firms use different techniques to control for bias, including some firms that exclude sensitive attributes like gender and race from model development and others that collect it in order to validate those models (*id.*, p.16). ML techniques have helped correct biases against minorities and women, particularly by improving the handling of data gaps and outliers. (*Machine Learning Thematic Series Part II: Bias and Ethical Implications*, May 2019, p.15). Many firms indicated that the use of ML had allowed them to understand and monitor the risk posed by each customer in a more holistic manner (*id.*)

Question 10: How are financial institutions addressing any increase in fair lending and other consumer-related risks, including identifying and addressing possible discrimination, related to the use of AI, particularly emerging AI technologies? What governance approaches throughout the development, validation, implementation, and deployment phases do financial institutions expect to establish to ensure compliance with fair lending and other consumer-related laws for AI models and tools prior to deployment and application? In what ways could existing fair lending requirements be strengthened or expanded to include fair access to other financial services outside of lending, such as access to bank accounts, given the rapid development of emerging AI technologies?

Addressing risks: Financial institutions are using a range of techniques to control bias risk, with the top three being auditing and testing, applying a code of ethics defined at the institutional level, and using a code of ethics specific to AI/ML (2023 survey report, p.15-16). Some institutions exclude features such as gender, race, and other sensitive attributes from the beginning to prevent them from being part of the feature analysis, selection, and engineering process (*ibid*, p.16). ML techniques have been found to "reduce the possibility of unlawful discrimination by helping ensure consistency and uniformity and minimizing individual judgment and discretion" in credit decisions (FDIC Supervisory Insights, "Fair Lending Implications of Credit Scoring Systems" (Summer 2005), cited in IIF, *Machine Learning Thematic Series Part II: Bias and Ethical Implications*, May 2019, p.9).

Governance: see answer to Question 8.

Suggestions on fair lending requirements: Our general remarks in the cover letter should be recalled here, particularly that the official sector should avoid layering on new regulations where there already are regulations addressing the same or cognate issues, particularly if existing regulations are not efficiently applied or enforced.

Question 11: How are financial institutions addressing any increase in data privacy risk related to the use of AI models, particularly emerging AI technologies?

Addressing increased privacy risk: The 2023 survey report mentions data privacy as a key ethical issue for AI/ML development and use. When considering the key ethical issues and core principles surrounding AI/ML development and use, a plurality of respondents selected privacy as their top

[24] See, for example, Machine Learning in Credit Risk (March 2018), p. 5, and Machine Learning in Credit Risk, 2nd edition: Summary Report (September 2019), p. 4.

concern (p. 12). Data risk management policies are applied extensively to manage GenAI risks (p.9). Specifically around GenAI risks, the 2023 survey report reports that 78% of respondents have or are in the process of establishing policies/procedures to control risks due to the use of GenAI, including data risk (p.9); and model risk management, compliance and legal risk, third-party risk, and data risk management policies are applied extensively to manage GenAI risks (p.9).

Question 12: How are financial institutions, technology companies, or third-party service providers addressing and mitigating potential fraud risks caused by AI technologies? What challenges do organizations face in countering these fraud risks? Given AI's ability to mimic biometrics (such as a photos/video of a customer or the customer's voice) what methods do financial institutions plan to use to protect against this type of fraud (e.g., multifactor authentication)?

We addressed payments security and trust in a September, 2023 staff paper on payments security and trust.[25] Losses to banks and their customers from increasing levels of fraud and scams, particularly authorized push payment (APP) scams, have recently attracted significant attention from policymakers and regulators. This increased attention prompted the IIF to convene an Asian region member roundtable on this topic on May 6-7, 2024. We draw on that staff paper and the discussion at that roundtable in the answers that follow.

Addressing and mitigating fraud risks: In response to the growing threat of AI-enhanced fraud, financial institutions and technology companies are implementing comprehensive strategies. These include the deployment of sophisticated AI-driven fraud detection and prevention systems capable of real-time analysis and pattern recognition. Advanced technologies such as voice cloning detection and phishing prevention are being integrated into existing security frameworks. Concurrently, these organizations are prioritizing education initiatives for both customers and employees, while fostering collaborative relationships with regulatory bodies, law enforcement agencies, and industry associations to exchange critical information and best practices. The utilization of third-party service providers offering multilayered security architectures further augments their defensive capabilities against evolving fraudulent tactics.

Challenges faced: The financial sector faces significant hurdles in combating AI-enhanced fraud. These challenges include the rapid advancement of sophisticated fraud techniques, necessitating substantial investments in cybersecurity infrastructure. A critical global shortage of cybersecurity professionals exacerbates the issue, with millions of positions unfilled, according to McKinsey (March 2022). The increasing realism of AI-generated scams, coupled with the proliferation of fraud-enabling tools on the dark web, further complicates detection efforts. These factors collectively underscore the complexity and scale of the evolving threat landscape in financial cybersecurity.

Methods financial institutions are using or planning to use to protect against AI-mimicked biometric fraud: Financial institutions are adopting multifaceted approaches to combat AI-mimicked biometric fraud. These strategies encompass advanced digital trust solutions, robust identity and access management systems, and adherence to comprehensive security standards. Institutions are also exploring national-level digital identity systems and leveraging AI for real-time anomaly detection. Additionally, they are implementing post-purchase anti-fraud measures and enhancing payment security through network token technologies. This diverse array of methods aims to create a more resilient defense against sophisticated biometric fraud attempts in an increasingly digital financial landscape.

Question 13: How do financial institutions, technology companies, or third-party service providers expect to use AI to address and mitigate illicit finance risks? What challenges do organizations face in adopting AI to counter illicit finance risks? How do financial institutions use AI to comply with applicable AML/CFT requirements?

Use of AI to address/mitigate illicit finance risks: Financial institutions, technology companies, and third-party service providers use, or expect to use, AI to address and mitigate illicit finance risks. In

[25] IIF (September 2023), IIF Staff Paper: Payments Security and Trust, pp. 7 – 9.

2022, institutions highlighted improving the efficiency of their models and discovering new risk segments/patterns as two key **benefits for their AML operations**. Furthermore, firms realized a reduction in false-positives through the use of machine learning and, in turn, a reduction in operating costs (2022 survey report, p. 7). AI processes complex datasets to create **more accurate risk profiles** of customers, enhancing customer due diligence and segmentation (*Machine Learning in Anti-Money Laundering Report*, October 2018, p.3). AI also improves **sanctions screening** processes, reducing both false positives and false negatives (*Payments Security and Trust: IIF Staff Paper*, September 2023, p. 10).

Challenges in adopting AI to counter illicit finance risks: Key challenges with launching AI/ML tools in production selected in the 2023 survey report were data quality, supervisory understanding or consent to use new processes, staff skillsets, underlying technology infrastructure, and explainability (p. 15).

Use of AI to comply with AML/CFT requirements: see our response to "Use of AI to address/mitigate illicit finance risks" above.

Question 14: As states adopt the NAIC's Model Bulletin on the Use of Artificial Intelligence Systems by Insurers and other states develop their own regulations or guidance, what changes have insurers implemented and what changes might they implement to comply or be consistent with these laws and regulatory guidance? How do insurers using AI make certain that their underwriting, rating, and pricing practices and outcomes are consistent with applicable laws addressing unfair discrimination?

Changes implemented to comply with NAIC bulletin: The NAIC AI Model Bulletin clarifies applicability of existing state laws that define and address unfair discrimination on the use of AI. In particular, underwriting and rating laws have not changed due to the adoption of the NAIC AI Model Bulletin, and insurers continue to comply with laws regarding the prohibition of the use of protected classes in rating and underwriting as well as the required transparency in filings and market conduct oversight.

Ensuring consistency with unfair discrimination laws: The 2023 survey report provides recent information on how financial institutions, including insurers, are addressing bias and discrimination. The top controls used by financial institutions to mitigate against bias and discriminatory outcomes are auditing, testing and controls, as well as applying a code of ethics defined at the institution level, and a specific code of ethics or equivalent for AI/ML (p.15). Some institutions exclude sensitive attributes like gender, race, and other protected characteristics from model development process and not used to evaluate bias, while for an equal number of respondents, features such as gender/race/sensitive are included in analysis and development and subsequently excluded from the model after assessing bias (p. 16). 78% of respondents have or are in the process of establishing policies/procedures to control risks due to the use of GenAI, including compliance and legal risk (p.9).

Question 15: To the extent financial institutions are relying on third-parties to develop, deploy, or test the use of AI, and in particular, emerging AI technologies, how do financial institutions expect to manage third-party risks? What challenges exist to mitigating third-party risks related to AI, and in particular, emerging AI technologies, for financial institutions?

Expectations for managing third-party risks: Based on the 2023 survey report, we can provide the following insights on how financial institutions expect to manage third-party risks related to AI.

1. Equivalent validation standards: 87% of respondents required third-party models to have the same level of validation as required for internally developed models (p. 2).
2. Risk management strategies: To manage third-party risks, institutions are asking for more developmental evidence from vendors and implementing compensating controls (p.2).
3. Governance frameworks: 78% of respondents have or are in the process of establishing policies/procedures to control risks due to the use of AI, including third-party risk. (p.9).

Challenges: As stated in our cover letter, financial institutions operate under prudential requirements that require FIs to develop their own sophisticated risk management governance frameworks, systems, and controls. FIs are constantly keeping such arrangements under review and making adjustments as needed, proactively. Such arrangements already apply to AI/ML systems operated by financial institutions. Based on the 2023 survey report, we can identify the following challenges in mitigating third-party risks related to AI for financial institutions:

1. Many of the latest innovations in GenAI have been driven by technology firms with large pools of data, so capabilities are often provided by third parties and deployed in the cloud. As a result, managing third-party risks is a prioritized area of focus (p. 1).
2. Challenges in validation: A majority within the 87% of respondents requiring third-party models to have the same level of validation as required for internally developed models noted challenges in obtaining requisite information to perform that same level of validation (p. 2).
3. Complexity of AI systems: Explainability/"black box" nature of some algorithms is the topic most identified as common/key issues raised during engagement on AI/ML models by respondents' regulator/supervisor, and bias and ethical issues related to the use of AI/ML was the second most identified topic (p.18).

These challenges highlight the need for financial institutions to develop robust strategies for managing third-party AI risks in an environment of rapid technological change and increasing complexity.

Question 16: What specific concerns over data confidentiality does the use of third-party AI providers create?

Our survey work does not provide specific information on data confidentiality concerns related to third-party AI providers. However, the 2023 survey report mentions that data privacy is the top ethical concern for AI/ML development and use (p.12).

Many institutions use third party cloud-based AI services. This could lead to the compromise of data security if there are flaws in cloud services or misunderstanding of the shared responsibility model under which most enterprise cloud services are provided. FIs need to put restrictions in place – either contractually or through cryptographic means – to prevent third parties from accessing and using any confidential data. This is a bigger issue now with GenAI – one reason why many firms blocked access initially to LLMs was due to concerns around how prompts could be used downstream for training the model and risk of data leakage.

One possible solution is to use technologies such as federated learning to reduce the risk of cross-organizational data usage. Other solutions including data encryption, access controls, data minimization, data anonymization, data tagging, auditing, and monitoring, employee training, and contractual safeguards.

In addition to data security issues, the use of third-party technology suppliers (including AI models) used in critical services can give rise to operational and other risks which need to be carefully managed. This issue, insofar as it concerns banks, is being considered by the Basel Committee on Banking Supervision and the IIF will contribute to that discussion.

Some FIs report that it is difficult to assess whether a third party's security practices truly meet their requirements and that they cannot validate the third party's internal processes.

Question 17: How are financial institutions applying operational risk management frameworks to the use of AI? How are financial institutions ensuring their operations are resilient to disruptions in the integrity, availability, and use of AI?

Applying operational risk management frameworks: The 2023 survey report indicates that:

1. 41% of institutions reported relying on existing model risk management or enterprise risk management frameworks for AI/ML application governance processes (p.10).
2. 25% of respondents are building new, complementary frameworks, and an additional 14% have already developed new, complementary frameworks for AI/ML applications (p.10).

3. 54% of the respondents use a tollgate process for proceed/don't proceed decisions in AI/ML use cases, with an additional 21% planning to introduce one (p.11).
4. 78% of respondents have or are in the process of establishing policies/procedures to control various risks due to the use of AI, including operational risk (p.9).

Ensuring resilience to disruptions: The IIF – EY survey series does not to date provide specific information on ensuring operational resilience to disruptions in AI systems. We would anticipate that operational resilience of AI/ML models is managed under our members' overall operational risk management framework (including that applicable to third party service providers). 66% of respondents have a C-suite officer overseeing AI/ML governance currently or are in the process of designating one, which could contribute to overall operational resilience (p.11).

Question 18: What actions are necessary to promote responsible innovation and competition with respect to the use of AI in financial services? What enhancements, if any, do you recommend be made to existing governance structures, oversight requirements, or risk management practices as they relate to the use of AI, and in particular, emerging AI technologies?

Actions necessary to promote responsible innovation and competition: Recent IIF staff work on cross-border payments identified examples of initiatives that could help incentivize adoption of advanced measures to address the challenges financial institutions face to payments security and trust, including challenges from AI, ecosystem complexity, and sanctions screening. Standardized data sharing gateways across borders and between sectors can also improve the power of AI-powered fraud and sanctions screening models, enabling customers to access a wider range of safe and secure payment products and services from different providers, while ensuring data protection and privacy (*Ibid.,* p. 11). Clarifying privacy regulation to enable data use to train sophisticated models, with client consent, can also improve the efficiency and accuracy of payments processing and fraud detection (*Ibid.,* p.13). Data standardization in sanctions screening and anti-fraud systems may also advance AI/ML more broadly (*Ibid.,* p. 13).

Recommended enhancements to governance / risk management:

The 2023 survey report suggests that the following may be helpful to financial institutions, depending on the extent to which they deploy or rely on AI/ML and on their business model, scale and complexity:

- implementing C-suite level oversight;
- establishing executive committees;
- implementing tollgate processes;
- establishing policies and procedures to control various risks due to the use of AI;
- developing new, complementary frameworks for AI/ML applications (*Ibid.,* p.10)

However, our members would caution that such arrangements should be kept flexible given the developing nature of AI/ML systems, and for this reason they consider there is no need for prescriptive regulation, beyond those that already apply in the regulated financial sector.

Question 19: To what extent do differences in jurisdictional approaches inside and outside the United States pose concerns for the management of AI-related risks on an enterprise-wide basis?

The IIF – EY survey series does not directly address the extent to which differences in jurisdictional approaches inside and outside the U.S. pose concerns for AI-related risk management on an enterprise-wide basis. However, some relevant points can be made building on existing IIF research on this topic.

For globally active firms, risk management is best conducted in possession of data from across the enterprise, ideally in real-time. Any data barriers or data "siloing", including data localization requirements, impose costs on enterprise risk management or make it less effective. The IIF staff paper *Data Policy Impacts - AML and Regtech Solutions* (March 2023) highlighted that advanced compliance (regtech) solutions, like many digital systems implemented by financial institutions, are increasingly reliant on new technologies, particularly cloud computing, AI and advanced data analytics. By their

nature such technologies are data-hungry, and their effectiveness can be impaired when high-quality, timely data is less available.

The IIF has consistently advocated against data localization rules that impair the effectiveness of risk management by reducing the data available to train AI/ML systems. Where there are data barriers, we have advocated for consideration to be given to setting out standardized gateways or exceptions, clarifying the circumstances under which authorities and FIs may make disclosures despite the presence of a data barrier.[26]

[26] In this regard, the IIF has proposed that data barriers could be addressed by providing a "gateway" or exception to facilitate the sharing of information by a business about local citizens or businesses (data subjects) where the business reasonably considers it necessary or expedient. See the IIF's January 14, 2022 response to the Financial Stability Board concerning the impact of data frameworks on cross-border payments, including case studies.

Annex II

Overview of 2023 IIF-EY 2023 Public Survey Report on AI/ML Use in Financial Services

The survey (**2023 survey report**) included a globally diverse group of 65 financial institutions, drawn from the IIF's membership, from across nine regions, responding to questions on AI/ML usage, governance and controls in financial institutions. Survey respondents included banks (G-SIBs, internationally active banks, national banks), insurers, and others (e.g., Central Bank, Brokerage, Asset Manager, Clearinghouse, Multilateral Organization).

The survey was conducted in June-August 2023. The key findings include that, as at the survey date:

1. **AI/ML Usage and Controls:** AI is being widely used in production, with 84% of respondents reporting usage of AI/ML techniques in production. Moreover, the numbers of use cases in inventory is large and growing, with only a narrow majority (52%) of respondent institutions having fewer than 50 AI/ML use cases in their current model inventory; 19% having 50-150 AI/ML use cases; 11% having 150-250 AI/ML use cases; 3% having 250-350 AI/ML use cases; and a full 15% having more than 350 AI/ML use cases in their current model inventory. Over the following three years, risk and compliance, operations, technology and data, and retail/consumer are predicted to be the most relevant areas of AI/ML usage for institutions surveyed. Most FIs already have policies/procedures to control risks or concerns related to model risk, data, technology, third parties, compliance and legal, operational, reputational, and business process continuity. The top two controls used by firms to mitigate against bias and discriminatory outcomes are auditing and testing.
2. **GenAI:** Financial institutions are increasingly integrating GenAI into their work. The overwhelming majority (86%) of respondents anticipate an expansion in their model inventories, with 40% of respondents expecting a substantial increase of over 20% in their entire inventory, and 46% anticipating a moderate expansion of around 20%. Respondents noted that near-term use cases include risk identification and assessment, code assistance, document querying and extraction, and financial crime/AML. All respondents in the U.S. and Asia Pacific (excluding Japan and China) impose at least some restrictions on the use of GenAI. 37% of respondents described the potential impacts of GenAI techniques as "revolutionary" on their business, indicating they see significant expansion in use cases ahead. As at the survey date, 100% of the FIs based in the U.S. expected to use GenAI primarily for internal deployments (non-customer facing) in the following 12 months. Globally, 81% of the firms had the same response.
3. **Benefits:** The 2023 survey report highlights that the top improved outcomes from using AI/ML techniques include the discovery of new risk segments and patterns, cost savings, and increased model accuracy. Institutions also reported benefits such as the ability to conduct holistic analysis of different data sources, more efficiency in the model development process, and overcoming data deficiencies or inconsistencies. These results chime with results from earlier surveys in the series: for credit risk management, increased model accuracy was overall the most improved outcome observed when using ML techniques globally in our 2022 survey on this topic. Discovery of new risk segments/patterns and the ability to conduct a holistic analysis of different data sources were commonly improved outcomes as well.[27] For AML, institutions highlighted two key benefits: improving the efficiency of their models and discovering new risk segments/patterns. Furthermore, firms realized a reduction in false-positives through the use of machine learning and, in turn, a reduction in operating costs.[28]
4. **AI/ML Governance, Oversight and Ethics:** Governance of AI/ML is well advanced, with 66% of respondents reporting a C-suite officer either currently or imminently responsible for AI/ML ethics and governance. A majority of respondents in the U.S., and half of respondents in Canada and Asia Pacific (excluding Japan and China) currently have such a manager in place,

[27] IIF and EY Survey Report on Machine Learning Uses in Credit Risk and AML Applications – Public Summary (December 2022).
[28] Ibid.

while all respondents in China currently have a C-suite officer responsible for AI/ML ethics and governance. Governance is also undergoing change: while 41% of institutions report relying on existing model risk management or enterprise risk management (ERM) frameworks, 39% have developed or are developing new frameworks for governing specific AI/ML applications. We are expecting even further progress in the governance of AI models in the 2024 results of our annual survey.

5. **Regulatory and Supervisory Engagement**: As regulatory interest in AI/ML intensifies, explainability and bias have emerged as the top issues in discussions with regulators. 53% of respondents have already engaged regulators/supervisors in the application of AI/ML techniques, and an additional 33% plan to do so within the next three years. Regulatory engagement seemed to be particularly important for U.S. institutions in 2023 – 88% of FIs based in the U.S. had already engaged regulators on the use of AI/ML. Furthermore, 57% of respondents noted that there are regulatory developments in their home jurisdiction that could impact their adoption of AI /ML.
6. **AI/ML Third-party Usage:** in 2023, a majority of survey respondents were expecting an increasing reliance on third-party AI/ML models over the 12 months following the survey. 87% of respondents require third-party models to have the same level of validation as required for internally developed models, but many highlight the challenge of obtaining requisite information to perform that same level of validation.

The 2023 IIF-EY survey paints AI/ML as experiencing a step-change in capability of underlying technology for the financial sector as financial institutions are reckoning with the potential, and associated risks, of GenAI developments this past year. The industry's focus on regulatory engagement and comprehensive governance structures underlines its commitment to responsible and innovative AI/ML deployment.