Submitted through regulations.gov

August 12, 2024

Moses Kim, Director, Office of Financial Institutions Policy
U.S. US Department of the Treasury
1500 Pennsylvania Ave., NW
Washington, DC 20220

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

Dear Director Kim:

Shared Assessments[1] is pleased to submit a response to the Request for Information ("RFI") on Uses, Opportunities, and Risks of Artificial Intelligence ("AI") in the Financial Services Sector (TREAS-DO-2024-0011-0001). As a membership organization that supports hundreds of companies and thousands of practitioners in third-party risk management (TPRM), Shared Assessments appreciates the opportunity to submit comments to those RFI questions that pertain to critical supply chain risk management, which are RFI questions 15, 16, and 17.

We hope that our comments to the RFI will contribute to the US Treasury and broader US federal government effort of creating greater clarity and regulatory harmonization in managing AI risks in the marketplace. If you would like to discuss any of our feedback further, please contact either of us at amoyad@sharedassessments.org or chrisjohnson@sharedassessments.org.

Sincerely,

Andrew Moyad
CEO
Shared Assessments LLC

Chris Johnson
Senior Advisor
Shared Assessments LLC

[1] Since 2005, Shared Assessments has been setting the standard in third-party risk assessments. Shared Assessments, which is the trusted source in third-party risk assurance, is a member-driven, industry-standard body that defines best practices, develops tools, and conducts pace-setting research. Program members work together to build and disseminate best practices and develop related resources that give all third-party risk management stakeholders a faster, more rigorous, more efficient, and less costly means of conducting security, privacy, and business resiliency control assessments, which include AI controls. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

15.1 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?

Financial institutions are increasingly relying on third parties to develop, deploy, or test AI technologies. Even where many of these companies have the resources to design, develop, and deploy AI technologies, speed to market concerns are driving an increasing number of them to license these services from third parties, as our own membership repeatedly advises us. (About 30% of our industry members are financial services firms, another 10% are insurance firms, and at least another 10% are technology/fintech companies that routinely develop or incorporate AI into their platforms.) To manage the associated range of third-party risks, financial institutions are implementing several strategies:

- Regulatory Compliance: Continued compliance with laws, rules, and regulations, including those that are not specific to AI but pertain to third-party risk management and, by extension, third-party AI technologies.
- Adherence to Guidelines: Ensuring that employees adhere to their third-party risk management guidelines, including all prohibitions on open code and data sharing.
- System Access Restrictions: Third-party service providers supporting AI programs/projects only have access to development systems. Production systems are highly restricted to ensure security and to minimize risk.
- Comprehensive Inventory: Maintaining an inventory of internal and third-party AI technologies that includes the name and technologies provided by third parties and other pertinent details. This inventory should be part of an integrated database that includes all AI-enabled and/or AI-production projects.
- Data and System Security: Ensuring data and system security by validating data and information output. (Increasingly, we find that many financial institutions are requesting software bills of material, or SBOMs, and there is a corollary and growing interest and evolving industry discussion in an AI equivalent, or AI-BOMs.)
- Clear Guidance and Contractual Safeguards: Revising and amending contracts to address AI risks explicitly. For instance: (1) third parties cannot use financial data in their models or open the code or systems to other parties using AI technology without permission; (2) outsourcer user data cannot be used for AI model training, and (3) contracts must provide for flexibility in anticipation of the ongoing evolution of AI security requirements.
- Expertise and Training: Hiring AI subject matter experts to document changing AI risks and provide appropriate training to internal and external stakeholders.

Considerations for US FIs Operating in the EU or UK

US financial institutions will need to comply with the EU AI Act and the guidance developed by UK authorities on AI.

- The EU AI Act requires providers and users to evaluate AI risks using a risk-based approach, classifying risks from “unacceptable” to “minimal”, and have appropriate governance and oversight structures to address key concerns.
- By the January 17, 2025, implementation deadline, the EU Digital Operational Resilience Act (DORA) requires US financial institutions operating in the EU to maintain an inventory of

information and communication technology (ICT) third parties, including those critical providers with AI-enabled services and the dependencies between providers among other third-party risk management and risk management measures. As stipulated under Article 8, Sections 3 and 5: (3) Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT-supported business functions, information assets, or ICT assets. (5) Financial entities shall identify and document all processes that are dependent on ICT third-party service providers and shall identify interconnections with ICT third-party service providers an undertaking providing ICT services that provide services that support critical or important functions (https://www.dora-info.eu/dora/article-8/).

15.2. How are financial institutions applying third-party risk management frameworks to the use of AI?

Financial institutions are increasingly integrating AI technologies into their operations, particularly in areas such as loan underwriting and credit risk management. To manage the associated risks, these institutions are applying robust third-party risk management (TPRM) frameworks. These frameworks ensure that AI technologies provided by third parties meet stringent regulatory and operational standards. By integrating TPRM with other risk management practices, financial institutions aim to mitigate potential risks, ensure compliance with regulations, and maintain the integrity and security of their systems.

One key approach involves leveraging Model Risk Management approaches into third-party sourced applications, particularly following guidelines such as SR 11-7 and OCC 11-12 for larger institutions and FDIC FIL-22-2017 for smaller institutions. This integration is crucial because third parties providing AI-based loan underwriting software are often deemed "Critical" within the TPRM program. These third parties are involved in essential functions and pose significant regulatory compliance risks. Consequently, institutions conduct enhanced due diligence during the initial vetting process. This process includes requests for quantitative studies to demonstrate a lack of bias, discrimination, redlining, and concentration risk. In some cases, Model Risk Management teams perform a special enhanced due diligence process on behalf of TPRM.

The presence or absence of transparency represents a significant risk-accepted aspect in the model validation process. There is also a notable focus on enhanced due diligence to ensure compliance and mitigate risks effectively. Explainability is another critical aspect of AI risk management. While banking customers seek transparency in AI models, the materials provided by third parties often fall short of supplying a clear understanding of AI capabilities, usage, targeted data, benefits, and related risks. Securing AI requires transparency, knowing how uses overlap with regulatory and other jurisdictional data handling and safeguard requirements, and promoting collaboration and information sharing among stakeholders (e.g., TPRM, Business Units, Compliance, Cybersecurity, Procurement, and Legal).

To address these challenges, financial institutions are updating their guidelines internally and externally regarding the use of AI. They are revising and amending contracts to address AI risks explicitly, such as prohibiting third parties from using financial data in their models or opening their code or systems to other parties using AI technology without permission.

Considerations for US FIs Operating in the EU or UK
Some financial institutions are using existing TPRM frameworks and measures and extending them to include AI, such as: (1) extending privacy impact assessments with AI questions to leverage that instrument as an AI impact assessment; and (2) mapping AI use among critical third parties to comply with EU Digital Operational Resilience Act (DORA) cyber resilience demands.

15.3. What challenges exist to mitigating third-party risks related to AI, and in particular, emerging AI technologies, for financial institutions?

Along with a general lack of expertise, experience, and often limited to no AI bench depth in their ranks, financial institutions face several challenges in mitigating third-party risks related to AI, particularly emerging AI technologies:

- Organizations often lack a clear understanding of how third and Nth parties are using AI, often without contractual obligations to notify them, raising concerns about potential impacts on their data, systems, and operations.
- A lack of harmonization in AI regulation across jurisdictions and industry frameworks to leverage (e.g., US NIST AI Risk Management Framework 1.0, January 2023) presents a challenge.
- Contractual obligations regarding AI use are often absent, particularly for evergreen contracts that lack amendments to address AI provisions. This results in the inability to ensure third parties adhere to outsourcer AI-mandated security hygiene obligations.
- Testing the resilience and response of third and Nth parties to cybersecurity threats and data protection issues is time-consuming, complex, and challenging.
- There is no guarantee of proper data usage, making it difficult to ensure that third parties, especially critical fourth parties, are handling data responsibly.
- Ethical issues and biases in AI outputs (algorithmic bias) are difficult to identify and mitigate, as well as instances of model poisoning, whether inadvertent or otherwise, adding another layer of complexity to risk management.
- Unauthorized access to biometric data can lead to identity theft and other forms of fraud, while misuse or bias in biometric AI systems can result in discriminatory practices and legal challenges.
- The use of AI models to analyze an organization's book of business and a potentially diverse set of uses for that information. Such uses may result in concentration risks specific to borrower types, geographies, product types, and monoculture risks as AI systems could potentially steer a business toward certain activities, products, and customer profiles, and negatively impact the organization's overall risk tolerance.
- There is significant concern about the lack of transparency and documentation of AI decision-making processes in credit denials, which is crucial for compliance and customer trust.
- Identifying and retaining resources skilled in AI, from technical management and optimization to risk professionals, is a significant hurdle.
- Companies providing AI technologies may not be familiar with and/or lack the resources to comply with evolving laws, rules, and regulations governing financial institutions.

Considerations for US FIs Operating in the EU or UK
Explainability of AI-Augmented Processes: Explainability is a key requirement in the EU AI Act and the UK guidance, but it can conflict with proprietary information that may be the unique selling

point of a provider. This conflict could expose financial institutions to AI risks associated with decisions either made by the AI model or made with human reliance on the AI model outputs that affect vulnerable populations, exclude clients on unclear grounds, flag transactions, and make chatbot suggestions due to AI hallucinations. Consequently, obtaining even high-level information about the AI model for oversight and EU AI Act compliance can be challenging if the provider is overly protective of trade secrets.

Managing Automation: The EU AI Act addresses concerns about automation in decision-making by stating that data subjects already have the right to opt-out under GDPR Article 22, which covers "Automated individual decision-making, including profiling." Similar efforts to protect data subject rights are underway in the US through the CCPA draft framework on “Automated-Decision-making Technology.” The act considers automated decisions as high-risk AI applications, especially in areas that could lead to automated exclusion from vital services or severely impact inclusion, such as automated credit checks, life insurance assessments, and recruitment: https://www.skadden.com/insights/publications/2024/05/uk-regulators-publish-approaches-to-ai.

Managing Consent: The EU GDPR has established a related requirement to identify the legal basis for any person or institution to process the personal information of data subjects (EU workers or EU residents), and that basis is very frequently driven by documented consent from the data subjects. However, as AI tools are commonly trained on personal information that may be organized, summarized, or even enhanced beyond its original use and the original basis for consent, financial institutions and their third parties have a newer, more complex challenge of ensuring and documenting that the original consent anticipated alternative uses such as AI or, worse, fail to meet the original conditions of the data subject’s consent and are not truly authorized.

Mapping Exposure to AI Risks: Organizations are already using high-risk AI applications that require stringent governance, human oversight, risk management, and documentation measures as demanded by the EU AI Act. Therefore, significant efforts are needed to assess the spread and risks of AI due to the heightened risk implications of automation.

15.4. How have these challenges varied or affected the use of AI across financial institutions of various sizes and complexity?

For some financial institutions, especially those with limited resources, the concerns around AI risks and the challenges of provisioning and preparing viable input training data have led to a cautious approach. As a result, some institutions are delaying plans to integrate AI into their operations until they can better understand and mitigate these risks. (However, even such anecdotally cautious approaches are often not reinforced or supplemented by written policies or technical measures to ensure all employees and other personnel honor the expected caution. Additionally, the freeware nature of many marketplace AI tools hardly stifles the curiosity of many staff who are eager to trial run or test AI tools in the marketplace, often in the absence of necessary policy and technical controls.)

With increasing AI use, financial institutions of all sizes are increasingly forced to reevaluate their risk tiering and risk acceptance criteria. This reevaluation is necessary to address the unique challenges posed by AI, such as ensuring the validity and accuracy of AI outputs and managing the

rapid pace of AI technology advancement compared to the slower evolution of regulations and organizational readiness.

Some institutions struggle with the lack of "tried and tested" outcomes, making it difficult for them to justify the investment in AI technologies without a clear understanding of the potential risks and benefits. Additionally, these institutions often face challenges in receiving timely notifications from third or fourth parties about AI usage, which further complicates risk management efforts across the ecosystem.

The use of technology for market entry is a double-edged sword for neobanks. While it facilitates their entry into the market, it also introduces new threat vectors and risks that need monitoring. This includes vulnerabilities in AI applications that could be exploited for intrusion, data exfiltration, and other malicious activities, potentially affecting customer data, funds, and transactions.

Considerations for US FIs Operating in the EU or UK
Large banks often have open banking arrangements with third-party providers, such as Payment Service Providers (PSPs) and Account Information Service Providers (AISPs), which may use AI in their services. For example, PSPs may use AI to detect fraudulent transactions in Open Banking/PSD2 arrangements and block critical transactions with an unexplained AI-assisted fraud management model. Further, if AISPs employ AI with lax controls, this could heighten the risk of data breaches for financial institutions and their clients that use AISP services that inadvertently expose client data or personally identifiable information through their application of AI.

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

The use of third-party AI providers creates several specific concerns over data confidentiality for financial institutions:

- Data Leakage: There is a significant risk of client data and proprietary strategies being leaked. Questions posed to the AI may inadvertently end up in outputs accessible to other users.
- Data Provenance: There is significant risk around sufficient understanding and control of data provenance, both with the source data associated with AI model training and the downstream AI result sets. In the absence of meaningful chain of custody data source tracking and controls, the provenance and integrity of AI results sets are potentially less reliable and certainly lack transparency in many cases.
- Re-Identification Risks: Lending models often use a wide range of factors that could potentially triangulate to specific individuals. As AI systems grow more sophisticated, there is a concern that previously anonymized or de-identified data could become identifiable, leading to a third party potentially having access to imputed PII (Personally Identifiable Information) data without proper controls.
- Lack of Control and Verification: Financial institutions often have no clear controls over how their data is being used by third parties. There is also no verification of whether the data were shared with additional parties, making it difficult to ensure that the data are secured and used appropriately.
- Unauthorized Access: There is a risk that data can be accessed by individuals who should not have access to it, leading to potential breaches and misuse of confidential information. Where

data has been used to train a model, the AI developer would have to revert the product to a version before that data is used to comply with privacy requirements for consumer right to delete (CCPA, Section 179-1830 and Section 1798.105. Consumers' Right to Delete Personal Information and GDPR).

- Potential Discrimination: The use of AI in lending models could lead to discrimination issues such as redlining and unfair lending practices. There is also a risk of over or underestimating earnings, which could negatively impact certain groups. Biased AI-based decision-making can also result in hiring discrimination in violation of EEO rules.
- General Third-Party Risks: The concerns with using third and Nth parties are not unique to AI but can be exacerbated by it. These risks include ensuring that only authorized personnel have access to data, implementing strong physical, technical, and operational controls, and managing the residual use of confidential data, such as for model training purposes.

Considerations for US FIs Operating in the EU or UK
The EU AI Act designates certain uses of AI as unacceptable and categorizes others as high risk. This restriction is not strictly about data confidentiality but focuses on the use of data for sensitive purposes, such as social scoring, law enforcement, and employment. Some high-risk or unacceptable AI risk categories in the EU AI Act could be enabled with publicly available information through methods such as "indiscriminate scraping of facial images" or categorizing individuals based on sensitive traits. Such information might be gathered from freely accessible sources like social media; however, individuals might expect that it will not be used for sensitive purposes such as recruitment or access to essential private and public services.

16.2 What *additional enhancements to existing processes do financial institutions expect to make in conducting due diligence prior to using a third-party provider of AI technologies?*

Financial institutions are enhancing their due diligence processes to address the unique challenges and risks posed by third-party AI providers. These enhancements include explicitly identifying AI-related risks and behaviors of concern, thoroughly understanding data collection, input fields, de-identification processes, and the potential for data triangulation to specific individuals; and as much as possible trying to mitigate those risks through contractual requirements.

Institutions are incorporating enhanced cybersecurity assessments and control testing into initial due diligence to ensure robust protection against threats. They are updating contractual provisions to clearly define the permissible use of AI by third parties, investing in training and hiring AI risk experts, and assessing the data security and controls implemented by third-party providers.

Considerations for US FIs Operating in the EU or UK
AI Impact Assessments are already being used to manage AI risks in Europe and are likely to be adopted by US financial institutions operating in the region.

16.3 *What additional enhancements to existing processes do financial institutions expect to make in monitoring an ongoing third-party relationship, given the advances in AI technologies?*

Given the advances in AI technologies, financial institutions are planning several enhancements to their processes for monitoring ongoing third-party relationships, but there is no consistent set of minimum practices or controls to establish an industry-acceptable standard of care, which will lead to uneven or incomplete adoption of good practices. That said, these enhancements in AI planning and programs are aimed at maintaining rigorous oversight and ensuring compliance, security, and risk management:

- Review and Monitoring: Institutions will adopt more aggressive review and monitoring practices to keep a close watch on third-party activities and AI usage. This due diligence is enhanced using specific contractual language reflecting AI-related concerns.
- Continuous Assessment of Loan Underwriting Models: Loan underwriting models run by third-party software need to be continuously assessed for Fair Lending violations, requiring some subset of the enhanced due diligence process to assess whether the model is free of bias or discrimination against any protected class factors must be periodically re-assessed quantitatively and qualitatively.
- Real-Time Intelligence: Ongoing monitoring programs will incorporate multi-category, real-time intelligence to keep pace with the dynamic capabilities of AI.
- Hiring AI Risk Experts: Financial institutions will invest in training and hiring AI risk subject matter experts to enhance their internal expertise and capability to monitor AI risks effectively. TPRM can leverage commonalities that allow the AI technology and the TPRM function to serve one another. AI models essentially create pseudo-experts, which can assist (augment) human experts in game-changing ways rather than replace those roles.
- Data Security and Controls: Continuous assessment of data security and controls will be necessary to ensure the protection of sensitive information.
- Resiliency Testing: Institutions will require proof of resiliency testing from third and fourth parties to demonstrate how they test and control their AI systems, ensuring stability and reliability.
- Compliance and AI Policies: Regular reviews and validations of compliance and AI policies of third-party providers will be conducted to ensure alignment with regulatory requirements and industry best practices.
- System Security Penetration Testing: Financial institutions will frequently review and validate the results of system security penetration testing to identify and mitigate potential vulnerabilities.

Considerations for US FIs Operating in the EU or UK

Subcontractor AI Deployment Alerts: In the EU and UK, contractual clauses often require third parties to inform clients of their use of subcontractors when there are material changes – which would likely include the deployment of AI.

Mapping the Use of AI: Financial institutions are expected to map the use of AI across the supply chain in line with the EU AI Act and the third-party inventory requirements of EU DORA.

Right to Audit: Article 30 of EU DORA is explicit about the right to audit third parties, granting "unrestricted rights of access, inspection, and audit by the financial entity." It is assumed that this extends to the audit of third-party AI providers and could also provide access to information about the AI technology that otherwise would not be made available.

16.4 *How do financial institutions manage supply chain risks related to AI?*

Financial institutions manage supply chain risks related to AI through several strategies aimed at ensuring robust oversight and risk mitigation, but these practices are not always consistent or consistently applied:

- Bilateral and Comprehensive Assessments: If there are other third parties providing data inputs used by an AI system provided by another party, a contractual relationship should dictate that those providers must be assessed both bilaterally and as part of the overall assessment of the primary AI system provider, particularly by independent parties (similar to today's best practice for cybersecurity testing programs). This approach ensures that all contributors to the AI system are scrutinized for compliance and risk.
- Internal Relationship Scope Governance: Institutions implement mapping processes across relevant AI service providers (direct and indirect) to ensure the vendor risk profile is accurate. This governance involves continuous, multi-category, real-time intelligence to keep pace with the changing risk landscape and expanded attack surface.
- Thresholds for Acceptable AI Usage: Establishing clear thresholds for acceptable AI usage by third and Nth parties is crucial. This helps in maintaining control over how AI technologies are used within the supply chain.
- Contractual Requirements: Contracts are revised to include specific AI language and approval requirements, address data ownership and use, and ensure effective controls over subcontractors and Nth parties. These contractual provisions need to be coupled with clear due diligence on governance frameworks, security practices, AI training controls, and data destruction processes.
- Approval and Notification Requirements: Third-party providers are required by contract to notify and obtain approval from the financial institution for any significant AI changes. This ensures that the institution remains aware of and can manage any changes that might affect risk.
- Resiliency Testing: Conducting regular resiliency testing is necessary to ensure that third-party AI systems can withstand and recover from potential disruptions.

Considerations for US FIs Operating in the EU or UK
US financial institutions operating in the EU may be required under DORA to document AI Impact Assessments and conduct ongoing assessments to remediate emerging AI risks and document those risks in the risk register required under EU DORA.

17.1 How are financial institutions applying operational risk management frameworks to the use of AI?

Financial institutions are integrating operational risk management frameworks to address the unique challenges posed by AI. They are adding AI-driven risks to their risk taxonomies and including them in recent risk identification exercises, which has led to updates in risk inventories. Although control design and testing processes for AI risks are still developing, there is an increased reliance on Risk and Control Self-Assessments (RCSA) to keep the risk profile current.

Institutions are enhancing guidelines to define acceptable AI usage more clearly, both internally and externally. This includes training employees and hiring AI risk subject matter experts to build

internal expertise. Establishing guardrails for AI usage and regularly testing AI outputs to ensure accuracy are also key strategies.

Furthermore, comprehensive risk management frameworks are being developed to consider the intended use of AI tools, model drift concerns, reputational impact, and compliance with state or federal regulations and best practices.

Considerations for US FIs Operating in the EU or UK
Institutions are updating their information security management systems, such as ISO 27001, to incorporate AI-related risks. Privacy Impact Assessments (PIAs), originally developed for CCPA and GDPR compliance, are being adapted to account for AI risks, reflecting attempts at more comprehensive privacy and data protection.

In terms of Business Continuity Management, institutions are updating ISO 23001 standards to address AI threats. This includes applying AI Impact Assessments (AIIAs) that build on existing PIAs and developing business continuity plans specifically for AI-related outages. Additionally, financial institutions are conducting scenario mapping for AI-induced disruptions to Important Business Services to comply with regulatory requirements like PRA SS1/21 in the UK.

17.2 What, if any, emerging risks have not been addressed in financial institutions' existing operational risk management frameworks?

Institutions have identified several emerging risks associated with AI technologies that are not currently addressed within their existing operational risk management frameworks. These unaddressed risks highlight the need for enhanced methodologies and increased awareness to effectively manage the complexities and uncertainties posed by AI:

- Regulatory Impacts: Institutions need to continuously monitor and adapt to any regulatory impacts that may arise from the evolving landscape of AI technology. The possibility of investments in AI technologies being rendered unusable by new legislation or rulemaking is a major concern.
- Machine Amplification of Errors and Biases: The potential for AI systems to amplify various hallucinations and fixed ideas stemming from poorly formulated questions and biased training is a significant risk. The level of incompetence and maliciousness in these scenarios can be much larger than anticipated.
- Monoculture Trajectory: There is a real potential risk of a monoculture trajectory developing over time in which a lack of diversity in AI models and approaches could lead to systemic vulnerabilities. However, this risk is challenging to define and to assess.
- IoT Impact: The proliferation of increased end-user tools and the Internet of Things (IoT) poses a risk that is not fully understood or managed within existing frameworks. This includes potential security vulnerabilities and data privacy issues. Shared Assessments research into TPRM and IoT documents little progress in managing IoT asset inventories and endpoint controls in ways that result in significant ongoing risk.
- Operational, Financial, and Customer Impact: There is a need for a comprehensive backup plan to identify, notify, review, escalate, and address the impacts of AI-related risks on operations, finances, and customers.

- Enhancements to Existing Methodologies: Existing risk methodologies should be enhanced to address AI risks in systems, including data collection, design of AI systems, and ongoing testing and monitoring. AI systems may require a redeployment of or additional resources to effectively monitor and test these systems.
- Disruptive Changes to Technology: Industry experts acknowledge that quantum attacks can result in AI applications, as they can in any other area.

Considerations for US FIs Operating in the EU or UK

An emerging risk that has not been fully addressed in existing operational risk management frameworks is the risk posed by PSPs and AISPs in the context of Open Banking. The growth of Open Banking in the US and Europe highlights the need for more attention to third-party risk, as open banking entities may facilitate critical services that could have wide systemic implications in the event of a payment flow disruption or other outage. AI technologies further increase threat vectors, such as account information breaches and re-identification, adding to operational and regulatory concerns.

17.3 How are financial institutions ensuring their operations are resilient to disruptions in the integrity, availability, and use of AI?

While resiliency has not been a major concern to date due to the presence of lateral human services that provide augmented inputs and signals to AI systems, this is an emerging risk. This concern is particularly relevant as banks begin to replace legacy staff in certain customer support and other functions with bots or other AI systems. Consideration should also be given to regulatory service levels regarding responsiveness (e.g., complaints, disputes):

- Employee Training: Institutions are investing in training employees to understand and manage AI systems effectively, ensuring they can handle disruptions and maintain operational continuity.
- Establishing Guardrails: Setting up clear guidelines and guardrails for AI usage helps maintain control over AI systems and ensures they operate within defined parameters.
- Testing AI Outputs: Regular testing of AI outputs is conducted to ensure their accuracy and reliability, which is crucial for maintaining trust in AI systems and their decision-making processes.
- Resiliency Testing: Both internal and external resiliency testing are performed to evaluate the robustness of AI systems and their ability to recover from disruptions. This includes stress testing and scenario analysis to prepare for potential issues.
- Alternative Supply Chains: Developing alternatives to current supply chains is essential. Institutions assess how quickly they can switch to alternative solutions, and the impact such changes would have on operations, financials, and customers. Alternative supply chain availability has become an increasingly important issue due to the rapid growth of concentration risk and the demonstrated ability of interruption at a single company to create widespread disruptions. Solutions to create the desired redundancy required for resilience are uniquely challenging and may require unprecedented, dedicated public-private sector cooperation.

Considerations for US FIs Operating in the EU or UK

Adherence with existing regulations that mandate managing of Important Business Services and Disruption Thresholds: Financial institutions are ensuring their operations are resilient to disruptions in the integrity, availability, and use of AI by adhering to regulatory requirements and implementing comprehensive risk management strategies. For example, US financial institutions operating in the UK are required to comply with PRA SS1/21, which mandates that they account for the tolerable disruption of Important Business Services (IBS) and remain within disruption thresholds by 2025. Additionally, institutions are establishing triggers for conducting AI Impact Assessments (AIIA) whenever there are material changes to AI models. These assessments help evaluate the potential impact of AI changes on operations and guide necessary adjustments to maintain resilience.

17.4 Are financial institutions using AI to preserve continuity of other core functions? If so, please provide examples.

AI is being employed to automate and reduce redundant tasks, allowing human employees to focus on more complex and value-added activities. This improvement in efficiency helps maintain continuity in operations. Additionally, AI can quickly scan and analyze documents, highlighting areas where human intervention is needed. This accelerates document review processes and ensures that critical issues are addressed promptly.

In data modeling, AI plays a crucial role by analyzing large datasets, identifying patterns, and generating insights that support decision-making processes. This capability is essential for maintaining the accuracy and relevance of financial models, the cybersecurity posture of institution networks and their supplier networks, as well as the ability to identify signals about institution and supplier geographic and operational risks and resilience.

Notably, financial institutions are increasingly leveraging AI-enabled cybersecurity solutions to identify and respond to cybersecurity threats more effectively, and this trend has continued over the last decade. These solutions enhance the continuity of core functions by proactively detecting and mitigating potential security vulnerabilities, threats, and even breaches, ensuring that systems remain secure and operational.