Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Financial Sector AI Deliverable Reference and Application Guide

The use of Artificial Intelligence (AI) and Generative AI (GenAI) offers tremendous opportunities within the financial sector including improving service delivery to customers and clients, strengthening fraud detection, increasing the security of firms themselves, and creating innovative products to grow the economy. Simultaneously, AI is also being used by nefarious actors to perpetuate fraud and weaken firms' security defenses. As AI continues to take hold, it is critical that financial institutions (Fis) use AI appropriately to maximize the positive impacts of this technology for their clients and customers, while also mitigating the risk of AI use by adversaries.

To better understand and address these dynamic concerns, in late 2024, the Financial Services Sector Coordinating Council (FSSCC)[1] and the U.S. Department of the Treasury (Treasury) in collaboration with the Finance and Banking Information Infrastructure Committee (FBIIC)[2] established the AI Executive Oversight Group (AIEOG). The AIEOG initiated six workstreams on:

- AI Lexicon and Taxonomy
- Financial Services AI Risk Management Framework
- Explainability
- Data-Nutrition Labeling
- AI Enhanced Fraud
- Identity and Authentication

This document provides an overview of the key deliverables and how organizations can use them. All of the AI deliverables can be found at https://fsscc.org/AIEOG-AI-deliverables/ .

Lexicon and Taxonomy

The Shared AI Lexicon and Taxonomy (Lexicon) defines key AI-related terms based on definitions from various industry standards and government resources with the goal of improving sector communications, on aspects ranging from risk management to contracts negotiation. Participants from FBIIC member federal agencies and FSSCC member firms collaborated with Treasury on the development of the Lexicon. The Lexicon includes common risk management and technical terminology with a focus on frequently used terms that have a specific meaning in the context of AI use in the financial sector.

[1] For more information on the Financial Services Sector Coordinating Council visit: https://fsscc.org/
[2] For more information on the Financial Markets, the Financial and Banking Information Infrastructure Committee visit: https://www.fbiic.gov/

Intended Audience/s: Agencies considering regulation in the AI space, technology risk management professionals, AI service provider product development teams.

Financial Services AI Risk Management Framework

The Financial Services AI Risk Management Framework (FS AI RMF) is an operationalization of the National Institute of Science and Technology's (NIST) AI RMF[3] specifically tailored for financial services. It is intended to be a practical, industry-backed tool that helps financial institutions effectively manage and govern AI-related risks. Its primary purpose is to foster consistent, responsible AI development, deployment, and use that aligns with existing regulatory expectations and industry standards, while still supporting innovation and efficiency.

The FS AI RMF consists of four primary deliverables—an AI Adoption Stage Questionnaire, a Risk and Control Matrix, a User Guidebook, and a Control Objective Reference Guide. It is designed as a complement rather than a replacement to existing frameworks and provides a scalable and adaptable approach tailored specifically for the financial services environment. Organizations can utilize the FS AI RMF to design and conduct their own assessments, address gaps, prioritize mitigation efforts, and develop a more resilient control posture across various stages of AI adoption.

Intended Audience/s: Financial firms' technology leaders and governance, risk, and compliance (GRC) and legal teams.

Explainability

Explainability has long been a cornerstone of model evaluation and testing in the financial industry. Traditional financial models provide clear and understandable rationales for their outputs, enabling stakeholder trust, ongoing monitoring and testing to ensure models operate as intended. The emergence of advanced, probabilistic Gen AI algorithms — now applied in areas such as fraud detection, cybersecurity, anti-money laundering, and customer support — holds significant promise for improving efficiency but also increases complexity in explainability. Strong governance and risk oversight are essential to maintain stakeholder confidence.

The goal of this paper is to foster responsible AI by integrating explainability into practice, effectively balancing capabilities and tool deployment, model and non-model performance,

[3] https://www.nist.gov/itl/ai-risk-management-framework

products, and services with transparency and control. Financial institutions are integrating five key disciplines: (1) Governance and Risk Management Frameworks, (2) Data Governance, (3) Prompting Guardrails, (4) Assurance and Testing, and (5) Ongoing Risk Monitoring and Outcome Analysis to foster improved explainability. These risk practices incorporate a series of cross-functional and multi-discipline policies, operating controls and standards of care that firms apply to ensure that Gen AI has tailored and rigorous review. Through use of these practices, firms will be able to accelerate innovation and ensure a competitive financial industry.

Intended Audience/s: Regulatory agencies, policymakers, and government bodies responsible for overseeing AI applications in banking and finance; data management and automation teams; governance, compliance, and risk teams.

Data Nutrition Labeling

The rapid integration of AI and GenAI across all industries further emphasizes the importance of having transparency and standards for the quality of data used for AI solutions. More specifically, the effectiveness and trustworthiness of GenAI systems is highly dependent on the quality and content of data used to train Large Language Models (LLM), including unstructured data. Lack of standards, transparency, and quality surrounding the use of data for GenAI systems can result in ineffective and potentially inaccurate GenAI systems. The Data Nutrition Labeling (DNL) paper recommends a more structured approach for the evaluation of data quality as it relates to AI solutions in the financial sector, to support increased transparency and trust in the use of AI. The integration of DNLs for financial institutions can address three issues:

1. Ensure the appropriate level of observability in data supply chains to support confidence and trust in leveraging AI and GenAI capabilities (near-term).
2. Drive standards across the sector to support enhanced transparency and explainability of AI and GenAI systems (medium-term).
3. Increase transparency and explainability in the use of AI and GenAI capabilities to enhance consumer confidence in Financial Institution's products and services (long-term).

By leveraging DNLs, FIs can remove ambiguity in the outcomes of their products, identifying risks inherent to the use of different types of datasets, and ensure alignment with state, federal, and international regulatory standards and guidance.

Intended Audience/s: Data management and automation practitioners, cybersecurity and fraud subject matter experts; governance, risk, and compliance teams.

AI Enhanced Fraud

Criminals are already using AI, especially generative AI, to supercharge familiar fraud and scam playbooks. FIs should plan and adapt now to mitigate AI to deceive consumers and employees. As these attacks evolve, most AI-enhanced fraud will be directed at consumers rather than the institutions themselves. This dynamic calls for a different institutional mindset: empowering consumers through continuous education, designing operations and communications to anticipate deception, modernizing incident response to include consumer-initiated fraud events, and evolving technology strategies to detect and disrupt these scams earlier in the engagement cycle.

This paper provides info on the AI Fraud Attack Landscape, details on what Education and Awareness programs should look like to counter these trends, Incident Response and Operational Reporting considerations, including how to respond to Deepfakes, Controls and Technology Responses, and a summary of how the ecosystem and sector is coming together to combat these issues together.

Intended Audience/s: Second line risk management teams, enterprise fraud operations teams, threat intelligence teams.

Identity and Authentication Workstream

Mitigating AI-powered threats to identity and authentication is now a critical focus for financial institutions. “Mitigating AI-Powered Attacks Against Identity and Authentication” outlines three primary attack vectors -- deepfake-driven social engineering and impersonation, synthetic identity creation, and AI agents as attack surrogates -- comprising of 10 specific tactics that threaten identity and authentication systems and mitigation strategies. The framework aligns each attack type with nine fraud scheme red flags identified by FinCEN, providing clear and actionable guidance for detection and response. The paper also includes a maturity model for identity controls to combat malicious use of Gen AI that lays out high-level technologies, ideas, and frameworks financial institutions can work towards mitigation of Gen AI-powered attacks.

“Recommendations for Policymakers: Mitigating AI-Powered Attacks Against Identity and Authentication” outlines 20 distinct actions for policymakers – spread across four key initiatives – that would collectively help FIs defend against current and emerging attacks powered by Gen AI that target FI identity and authentication systems. The paper includes a

rationale for how each of these initiatives would help financial institutions defend against Gen AI-enabled attacks. The four initiatives are: prioritize the development of next-generation remote identity proofing and verification systems; promote and prioritize the use of strong authentication; coordinate with other countries and harmonize requirements; and educate consumers and businesses about better identity and emerging identity threats. Intended Audience/s: Enterprise fraud operations teams, Customer Identity and Access Management teams, technology risk teams, Retail bank LOB, and security personnel for incorporation of identity-SAR based trends mitigation training. Policymakers at US Government agencies — both regulatory and non-regulatory — and in legislative bodies who play a role in safeguarding the financial services sector and other critical infrastructure sectors from the risks posed by Gen AI.

Intended Audience/s: Customer identity and access management teams, enterprise fraud operations teams, threat intelligence teams.

The latest AIEOG documents exemplify the financial sector's collaborative efforts with public partners to responsibly integrate technology and manage third party service providers. These most recent documents add to the suite of prior guidance from the Cloud Executive Steering Group on the secure integration of Cloud technology. Key resources that may be helpful to financial institutions still migrating to the cloud include:

- The Financial Sector Cloud Outsourcing Issues and Considerations document, which addresses transparency, operational risk, resource gaps, and contract negotiation issues.
- The Cloud Profile 2.0, which extends the NIST-based Cybersecurity Profile to provide a practical cloud security implementation plan for diverse financial institutions.
- The Transparency and Monitoring for Better "Secure-by-Design" document, which offers a service inter-dependency and resilience model alongside baseline security outcomes for cloud workloads.

Collectively, these documents furnish actionable tools and expectations that empower financial institutions of all sizes to securely adopt cloud services, enhance operational resilience, and meet evolving regulatory standards. The cloud deliverables can be found at https://fsscc.org/fsscc-cesg-cloud-group-deliverables/ .