Just in Time

In Data We Trust? Emerging Policy and Supervisory Approaches to AI Data Use in Financial Services

April 2026

iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

Executive Summary

The paper [1] examines the **centrality of data in AI systems within financial services**, highlighting how the rapid adoption of advanced AI - particularly generative AI (gen AI) - has amplified both the **importance and risks of data governance**.

Data are foundational across the entire AI lifecycle: they determine model training, influence outputs, and shape performance evaluation. However, the financial sector faces **structural data challenges**, including fragmentation, inconsistent quality, and reliance on legacy systems. These issues are intensified by gen AI, which requires **large, diverse and often unstructured datasets**, including alternative and synthetic data.

The paper underscores that while **cross-sectoral data protection frameworks** (e.g. privacy laws) provide a foundation, they are **not fully adapted to AI-specific challenges**, especially across different lifecycle stages. The paper that **further supervisory guidance is required**, particularly on: Data lifecycle governance; Third-party risk management; Data lineage and transparency; Integration of cybersecurity and data protection.

[1] *BIS-FSI, "In data we trust? Emerging policy and supervisory approaches to AI data use in financial services", March 2026*

At a Glance

Keywords: AI, GenAI, Data Governance, Data Quality

01

Introduction

Overview

Introduction

Overview

The AI is a **transformational force in financial services**, with data as its core enabling input.

Financial institutions rely heavily on data to perform essential functions such as credit allocation, risk management, and payments processing. With the emergence of gen AI, these processes are becoming more **automated, scalable and complex**, increasing both opportunities and risks.

A central premise is that **data quality directly determines AI performance**. Poor-quality data can lead to **inaccurate, biased or harmful outcomes**, especially in high-stakes applications like credit underwriting:

- Data in AI systems often include **personal and sensitive information**, subject to strict regulatory requirements;
- Compliance with data protection laws is becoming **more complex due to AI's scale and opacity**;
- Data-related challenges are consistently identified as **primary barriers to AI adoption** globally.

Supervisory authorities face a dual challenge:

- Monitoring risks from AI use by financial institutions;
- Addressing **data governance issues that extend beyond traditional supervisory mandates**.

It is important **to clarify emerging supervisory expectations** and identify **common regulatory themes across jurisdictions** (China, EU, Singapore, UK, US).

02

The Role of Data in AI and the Financial Sector

Background and Use of Data in AI Systems

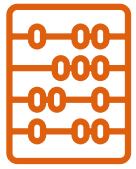
Data Challenges in AI Systems

The Role of Data in AI and the Financial Sector 1/2

Background and Use of Data in AI Systems

Background

Financial services are inherently **data-driven**, relying on structured, semi-structured and unstructured data from multiple sources, including:



- Internal systems;
- Third-party providers;
- Alternative data (eg digital footprints);
- Synthetic data.

A key distinction is made between:

- **Personal data**, subject to data protection frameworks;
- **Non-personal data**, with fewer restrictions but increasing regulatory attention.

The growing role of **privacy-enhancing technologies (PETs)**, such as anonymisation and differential privacy, while noting their **trade-offs between privacy and data utility**.

Use of Data in AI Systems

Data underpin every stage of the **gen AI lifecycle**, including:

- Training;
- Testing;
- Fine-tuning;
- Deployment and monitoring.

The paper identifies **three key stakeholders**:

- **Data providers** (internal and external);
- **Model developers** (often third-party tech firms);
- **Model deployers** (financial institutions).

The lifecycle approach emphasises that **data risks are dynamic and cumulative**, evolving across stages.

The Role of Data in AI and the Financial Sector 2/2

Data Challenges in AI Systems

Core risk categories

- **Data quality risks**: inaccuracies, bias, data drift;
- **Privacy risks**: misuse, unintended disclosure, profiling;
- **Security risks**: cyberattacks, data poisoning, prompt injection.

Amplified risks from gen AI

Gen AI exacerbates existing issues and introduces new risks:

- Increased reliance on **large-scale heterogeneous data**;
- Greater exposure to **bias and inaccuracies**;
- Challenges linked to **synthetic and alternative data**.

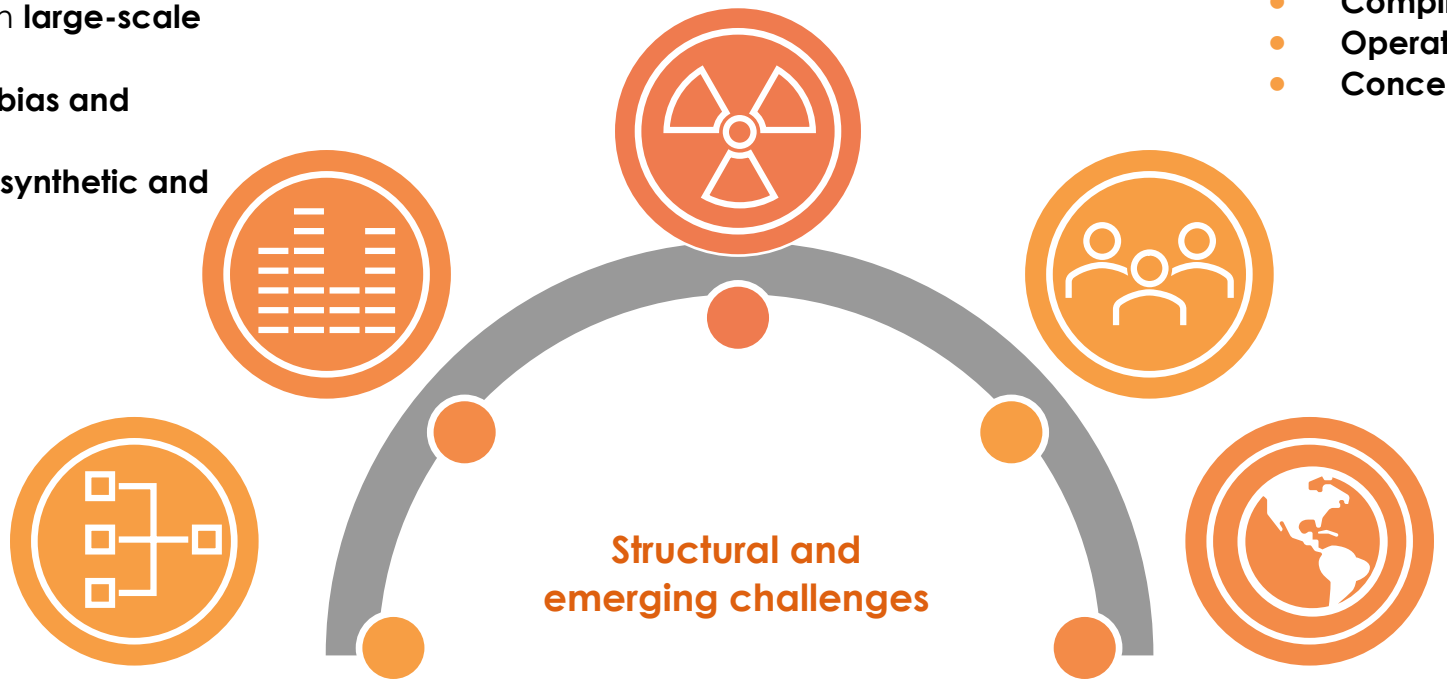
Third-party dependencies

Reliance on external providers reduces transparency and increases:

- **Compliance risk**;
- **Operational risk**;
- **Concentration risk**.

Fragmentation and legacy systems

Financial institutions operate with **siloed and inconsistent data architectures**, limiting interoperability and data quality.



Systemic implications

Data shortcomings may lead to:

- Consumer harm;
- Weakening of risk models;
- Increased **herding behaviour and systemic risk**.

03

Key Themes in Cross-Sectoral Guidance on Use of Data in AI

Data Privacy, Fairness and Transparency

Data Quality, Data Security, Data Governance

Key Themes in Cross-Sectoral Guidance on Use of Data in AI 1/2

Data Privacy, Fairness and Transparency

Cross-sectoral data protection frameworks, identifying some core pillars:

a. Data Privacy

Data privacy is defined as **individual control over personal data**, operationalised through legal frameworks.

Key principles include:

- **Lawful basis** (eg consent, legitimate interest);
- **Purpose limitation**;
- **Data minimisation**;
- **Retention limitation**.

Challenges in AI:

- Difficulty obtaining meaningful consent;
- Tension between **large data needs and minimisation requirements**;
- Ambiguity in lawful use of publicly available data.

Data subject rights, include:

- Access;
- Rectification;
- Erasure;
- Objection;
- Protection from automated decision-making.

These rights are **difficult to implement in AI**, particularly due to:

- Lack of transparency in training data;
- Model memorisation;
- Limited control by deployers.

b. Fairness and Transparency

Fairness requires avoiding **bias and discriminatory outcomes**, while transparency requires **clear disclosure of data use**.

Challenges:

- AI models are often **non-explainable ("black box")**;
- Trade-offs between **transparency and intellectual property protection**;
- Difficulty detecting embedded bias.

Key Themes in Cross-Sectoral Guidance on Use of Data in AI 2/2

Data Quality, Data Security, Data Governance

Cross-sectoral data protection frameworks, identifying some core pillars:

c. Data Quality

Data quality is central to both **data protection and AI frameworks**, focusing on:

- Accuracy;
- Completeness;
- Representativeness.

The paper highlights a **conceptual divergence**:

- Data protection: correctness of personal data;
- AI: probabilistic accuracy based on predictions.

Supervisory expectations emphasise:

- Continuous quality assurance;
- Lifecycle monitoring;
- Responsibility of both developers and deployers.

d. Data Security

Data security encompasses:

- Confidentiality;
- Integrity;
- Availability.

AI increases exposure to:

- Cyberattacks;
- Data breaches;
- Operational disruptions.

Strong security controls are essential for **operational resilience and trust**.

e. Data Governance

Data governance is the **foundational framework** integrating all other elements.

It includes:

- Roles and responsibilities;
- Policies and processes;
- Accountability mechanisms.

Governance is critical to ensure:

- Compliance;
- Traceability (data lineage);
- Effective risk management.

04

Financial Sector-Specific Guidance

Reference Frameworks, Supervisory Approaches and Challenges Identified

Financial Sector-Specific Guidance

Reference Frameworks, Supervisory Approaches and Challenges Identified

Financial authorities build on cross-sectoral frameworks but adopt **sector-specific supervisory approaches**.

Reference frameworks

Key frameworks include:

- **BCBS 239** (risk data aggregation and reporting);
- Model risk management frameworks;
- Operational resilience and outsourcing guidelines.

These frameworks are **technology-neutral but applicable to AI**.

Supervisory approaches

Authorities use a combination of:

- **Existing regulations** (adapted to AI);
- **Non-prescriptive tools**, such as:
  - Thematic reviews;
  - Supervisory statements;
  - Best practice guidance.

Emerging supervisory focus areas:

- Data governance frameworks;
- Data quality standards;
- Cybersecurity integration;
- Third-party risk management.

Challenges identified

- Lack of **AI-specific supervisory consistency**;
- Difficulty applying existing rules to **gen AI complexity**;
- Limited visibility into **third-party data ecosystems**;
- Regulatory fragmentation across jurisdictions.

05

Conclusions and Take-aways

Conclusions and Take-aways

AI data risks are not fully addressed by existing frameworks, requiring **targeted policy evolution**.

Key recommendations include:

- Development of **AI-specific data governance guidance**;
- Strengthening **data quality and security expectations**;
- Enhancing oversight of **third-party dependencies**;
- Promoting **data lineage transparency**.

The paper stresses the importance of:

- **Cross-border regulatory cooperation**;
- Coordination between **financial and data protection authorities**;
- Continuous dialogue with industry.

The overarching goal is to ensure that AI adoption:

- Supports innovation;
- Preserves **trust and consumer protection**;
- Strengthens **financial stability**.

Strategic implications for financial institutions

- AI adoption is not just a technology issue—it is a **data governance transformation challenge**
- Institutions must:
  - Invest in **data infrastructure and quality**
  - Strengthen **governance frameworks**
  - Enhance **cross-functional oversight (risk, IT, compliance)**

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

KEEP IN TOUCH

iason

Company Profile

iason is an international firm that consults Financial Institutions on Risk Management. **iason** integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Dario Esposito

Tommaso Travenzoli

Enrico Ferro

Matteo Bazzucchi

www.iasonltd.com