

Just in Time

Sound Practices for Responsible Adoption of Artificial Intelligence

July 2026



Executive Summary

- The Financial Stability Board (FSB) issued this **consultation report** to establish a globally consistent set of **sound practices for the responsible adoption of Artificial Intelligence (AI)** by financial institutions. The initiative responds to the rapid acceleration of AI deployment across the financial sector, particularly following recent advances in **Generative AI (GenAI)** and **Agentic AI**, which have significantly expanded the capabilities of machine learning systems.
- The FSB is inviting comments on this consultation report and the questions set out within it: **responses should be submitted by 22 July 2026.**
- FSB, Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Consultation report, June 2026



At a Glance

01	<u>Introduction</u>	4
02	<u>Overview of the Use of AI in the Financial System</u>	7
03	<u>Organisation-Wide AI Governance</u>	12
04	<u>AI Lifecycle Management</u>	15
05	<u>Conclusions & Take-aways</u>	18

Keywords: Technology, AI, AI Risk Management



01

Introduction



Introduction 1/2

The FSB report acknowledges that AI is no longer an experimental technology within financial services. **Banks, insurers, asset managers, payment service providers, and financial market infrastructures** are **increasingly embedding AI into critical business functions**. AI is being used to automate routine tasks, support complex decision-making, enhance customer engagement, improve operational efficiency, strengthen risk management capabilities, and bolster cyber resilience.

The FSB recognises that AI adoption offers substantial **benefits**, including **productivity gains**, **cost reductions**, improved **risk detection**, and **enhanced customer service**.

However, these benefits are accompanied by **new** and evolving **risks** that, if not properly managed, could undermine the safety and soundness of individual institutions and potentially affect financial stability.

Rather than introducing a binding international standard, the FSB proposes a **principles-based and technology-neutral framework**.

➤ The report explicitly **avoids prescribing specific technologies or business models**. Instead, it provides a menu of **twelve sound practices** that institutions may adopt proportionately according to their size, complexity, interconnectedness, and the materiality of AI use cases.

➤ A central theme throughout the report is **proportionality**. Large internationally active financial institutions operating AI in critical business functions are expected to implement more sophisticated governance, risk management, and control frameworks than smaller institutions using AI for limited operational purposes.

Introduction 2/2

The proposed **framework** is organised around **two pillars**:

Organisation-Wide Governance

The first **four sound practices** focus on enterprise-level governance, covering:

Strategic oversight by boards and senior management

Accountability and governance structures

Integration of AI risks into existing risk management frameworks

Organisational learning and adaptability

The report emphasises that **responsible AI adoption** is not solely a technology issue. It requires strategic leadership, organisational culture, effective governance, and continuous adaptation as AI technologies evolve.

AI Lifecycle Management

The remaining **eight sound practices** focus on managing AI throughout its lifecycle, including:

Materiality assessments

Performance monitoring

Model selection

Human oversight

Data governance

Cybersecurity

Explainability

Third-party risk management

The FSB also highlights the importance of **collaboration** among regulators, supervisors, technology providers, and financial institutions to ensure that innovation can proceed while maintaining trust, resilience, and financial stability.

02

Overview of the Use of AI in the Financial System

AI Adoption across Financial Services

Key Use Cases and Benefits

Risks and Challenges



Overview of the Use of AI in the Financial System 1/4

AI Adoption across Financial Services 1/2

The report observes that AI adoption has accelerated significantly since the FSB's 2024 assessment of AI-related financial stability implications.

Several **factors** are **driving adoption**:



Supply-Side Drivers

Increased computing power

Cloud infrastructure availability

Expansion of accessible data

Emergence of foundation models

Reduced implementation costs



Demand-Side Drivers

Competitive pressures

Operational efficiency objectives

Enhanced customer expectations

More sophisticated risk management needs

Digital transformation initiatives

Overview of the Use of AI in the Financial System 2/4

AI Adoption across Financial Services 2/2

The report notes **significant variation** in adoption rates across **sectors** and **jurisdictions**.

Banking Sector	Insurance Sector	Asset Management and Capital Markets	Payments Sector	Financial Market Infrastructures (FMIs)
Banks are among the most advanced adopters of AI, particularly in: • Credit risk management; • Fraud detection; • Compliance; • Document processing; • Internal productivity tools. While AI is increasingly used in front-office activities, banks remain cautious regarding fully automated decision-making due to explainability and regulatory concerns.	Insurers are applying AI to: • Claims processing; • Underwriting; • Customer segmentation; • Fraud identification. Traditional rule-based approaches are increasingly being supplemented by AI-driven methodologies.	Asset managers and trading firms use AI for: • Portfolio optimisation; • Algorithmic trading; • Market surveillance; • Sentiment analysis; • Liquidity forecasting; • Volatility modelling. Although autonomous trading remains limited, firms are actively exploring agentic AI applications.	AI has become central to: • KYC verification; • Fraud prevention; • Transaction monitoring; • Customer onboarding. Institutions report improvements in both processing speed and detection accuracy.	FMIs are deploying AI for: • Settlement optimisation; • Reconciliation; • Market monitoring; • Stress testing; • Early warning indicators.

Overview of the Use of AI in the Financial System 3/4

Key Use Cases and Benefits

The report identifies **several high-impact use cases**.

Credit Risk Assessment	Trading and Portfolio Management	AML, KYC and Fraud Detection	Customer Engagement	Productivity Enhancement	Operational Resilience
AI enables lenders to analyse: - Traditional financial data; - Alternative datasets; - Behavioural information; - Cash flow patterns. Benefits include: - Improved risk segmentation; - Lower default rates; - Enhanced SME lending; - Expanded financial inclusion. Several institutions report substantial reductions in credit underwriting times through GenAI-enabled automation.	AI supports: - Signal extraction; - Market analytics; - Research automation; - Portfolio construction. Benefits include: - Improved efficiency; - Faster decision-making; - Discovery of new investment opportunities.	AI strengthens financial crime controls through: - Real-time transaction monitoring; - Pattern recognition; - Anomaly detection; - Identity verification. Institutions report: - Lower false positives; - Improved detection rates; - Faster investigations.	AI-driven tools enhance: - Customer support; - Financial advice; - Marketing; - Complaint management. Chatbots and virtual assistants have become widely adopted.	GenAI applications are increasingly used internally for: - Coding assistance; - Research; - Drafting; - Knowledge management; - Documentation. Many institutions report significant productivity gains.	AI is helping institutions: - Detect cyber threats; - Monitor networks; - Respond to incidents; - Strengthen business continuity.

Overview of the Use of AI in the Financial System 4/4

Risks and Challenges

The report stresses that **AI risks** are becoming **increasingly significant**.

Governance Failures	Without effective oversight: • Accountability may become unclear; • Risks may go unmanaged; • Shadow AI usage may proliferate.	Data Risks	Poor data quality can lead to: • Bias; • Inaccurate decisions; • Regulatory breaches; • Weak model performance.	Explainability Challenges	Complex AI systems often function as "black boxes", creating difficulties in: • Validation; • Auditability; • Regulatory compliance; • Understanding causal relationships.	Model Performance Risks	Potential issues include: • Hallucinations; • Data drift; • Model drift; • Failure under changing conditions.	Consumer & Market Conduct Risks	Inadequate guardrails may lead to: • Insufficient disclosure; • Unfair treatment; • Mis-selling; • Unsuitable advice; • Weak redress.
Human Oversight Risks	Overreliance on AI may weaken human judgement and reduce effective challenge.	Cyber Risks	AI can both enhance and amplify cyber threats through: • Prompt injection; • Model poisoning; • Deepfakes; • Automated attacks; • Vulnerability exploitation.	Third-Party Dependencies	The report identifies growing reliance on: • Cloud providers; • Foundation model developers; • Hardware suppliers. These dependencies may create concentration risks and systemic vulnerabilities.	Agentic AI Risks	Agentic AI introduces unique concerns: • Autonomous decision-making; • Unauthorised actions; • Data leakage; • System disruption; • Difficulty of human intervention.		

03

Organisation-Wide AI Governance



Organisation-Wide AI Governance 1/2

The FSB identifies **governance** as the foundation of responsible AI adoption.

Strategic Direction and Oversight

Boards and senior management must:

- Align AI adoption with business strategy;
- Define acceptable risk boundaries;
- Approve governance frameworks;
- Monitor implementation.

The report emphasises that **AI strategy should not be delegated solely to technology teams**. Boards should receive **management information** covering:

- AI deployments;
- Risk exposures;
- Incidents;
- Performance metrics;
- Strategic outcomes.

AI considerations should also be integrated into the **institution's risk appetite framework**.

Governance and Accountability

Institutions should establish:

- Clear ownership structures;
- Defined roles and responsibilities;
- Cross-functional coordination mechanisms.

The FSB recommends **leveraging existing governance frameworks**, including the **three-lines-of-defence model**.

Effective governance requires **coordination** among:

- Business units;
- Risk functions;
- Compliance teams;
- Legal departments;
- Technology specialists;
- Internal audit.

Organisation-Wide AI Governance 2/2

AI Risk Management Framework

AI-related risks should be incorporated into **enterprise risk management processes**.

Institutions should:

- Identify AI use cases;
- Assess materiality;
- Document risks;
- Monitor performance;
- Apply proportionate controls.

Comprehensive **inventories of AI systems** should be maintained, including:

- Purpose;
- Risk classification;
- Dependencies;
- Data sources;
- Validation results;
- Ownership.

Organisational Adaptability

The report strongly emphasises **continuous learning**.

Institutions should:

- Develop AI literacy;
- Train staff;
- Enhance technical expertise;
- Promote a risk-aware culture.

Boards and management should remain informed about:

- Emerging technologies;
- Regulatory developments;
- Industry practices;
- New risk patterns.

The report highlights **public-private collaboration initiatives**, including AI sandboxes and industry consortia, as **important mechanisms** for organisational learning.

04

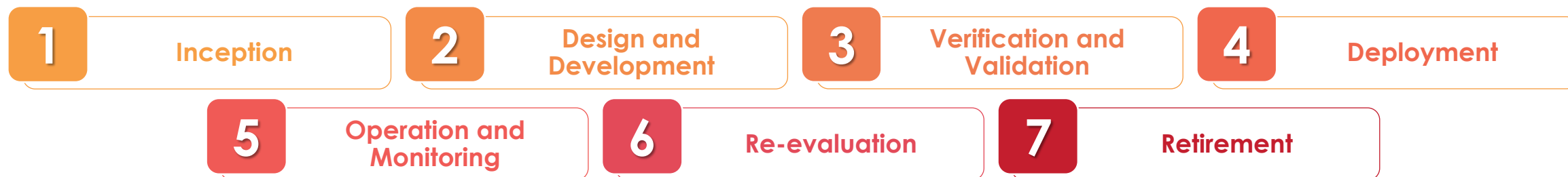
AI Lifecycle Management



AI Lifecycle Management 1/2

Just in Time

The FSB proposes a **lifecycle approach** to AI risk management. The lifecycle consists of:



Throughout these stages, **institutions should implement proportionate controls.**

Materiality and Risk Assessment	AI use cases should undergo structured assessment before deployment. Factors include: • Financial impact; • Customer impact; • Legal implications; • Operational criticality; • Degree of autonomy. Higher-risk use cases require stronger controls.	Selection	Institutions should select AI models based on: • Business objectives; • Technical suitability; • Risk characteristics; • Explainability requirements. The report cautions against adopting advanced AI solely because it is technologically attractive.	Data Governance	Data governance is identified as a critical success factor . Institutions should ensure data is: • Accurate; • Complete; • Reliable; • Secure; • Representative. Data controls should apply throughout the AI lifecycle.
--	---	------------------	--	------------------------	---

AI Lifecycle Management 2/2

Just in Time

Explainability and Transparency

The FSB recognises that **explainability varies across AI technologies**.

Institutions should:

- Understand model behaviour;
- Communicate limitations;
- Use more explainable models where appropriate;
- Implement compensating controls when explainability is limited.

Performance Management

Performance monitoring should include:

- Accuracy testing;
- Robustness assessments;
- Drift detection;
- Ongoing validation.

Testing should be **proportionate** to **materiality** and **risk**.

Human Oversight

Human oversight remains essential.

Controls should reflect:

- Complexity;
- Autonomy;
- Materiality;
- Explainability.

Human reviewers must have authority to intervene, challenge, or override AI outputs.

Cyber and ICT Risk Management

Institutions should **incorporate AI-specific scenarios** into cyber resilience programmes.

Key controls include:

- Security testing;
- Threat monitoring;
- Incident response planning;
- Information sharing.

Third-Party Risk Management

Third-party AI providers introduce unique challenges. Institutions should **assess**:

- Vendor transparency;
- Data governance;
- Operational resilience;
- Concentration risk;
- Business continuity arrangements.

The report places particular emphasis on **foundation model providers** and **cloud service concentration**.

05

Conclusions & Take-aways



Conclusions & Take-aways 1/2

Strategic Messages

- AI adoption is rapidly transforming the financial sector.
- **Benefits** include **productivity gains**, **enhanced risk management**, **improved customer service**, and **stronger operational resilience**.
- AI-related risks must be **managed through governance** rather than avoided through inaction.

Governance

- **Boards** and **senior management** are ultimately accountable for AI adoption.
- AI risks should be integrated into **enterprise risk management frameworks**.
- Clear **governance structures** and **accountability mechanisms** are **essential**.

Risk Management

- **AI lifecycle management** should be implemented end-to-end.
- **Materiality assessments** should drive proportionality.
- **Human oversight** remains critical, particularly for **high-risk use cases**.

Emerging Risks

- **Explainability challenges** remain significant.
- Agentic AI introduces **new governance** and **control requirements**.
- **Cybersecurity** and **third-party concentration risks** require heightened attention.

Regulatory Implications

- The FSB advocates a **technology-neutral and risk-based approach**.
- Institutions should remain **adaptable** as AI technologies evolve.
- **Collaboration** between supervisors, regulators, technology providers, and financial institutions will be essential.

Conclusions & Take-aways 2/2

Just in Time

The Twelve Sound Practices in Summary

- | | |
|---|------------------------------------|
| 1 Strategic direction and oversight. | 7 Data governance. |
| 2 Governance and accountability. | 8 Explainability and transparency. |
| 3 Integration of AI risks into risk frameworks. | 9 Performance management. |
| 4 Organisational adaptability. | 10 Human oversight. |
| 5 Materiality and risk assessment. | 11 Cyber and ICT risk management. |
| 6 Appropriate model selection. | 12 Third-party risk management. |

These twelve practices form the FSB's proposed framework for **responsible AI adoption in the global financial system**, aiming to balance innovation, operational efficiency, consumer protection, prudential soundness, and financial stability.

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**)

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.

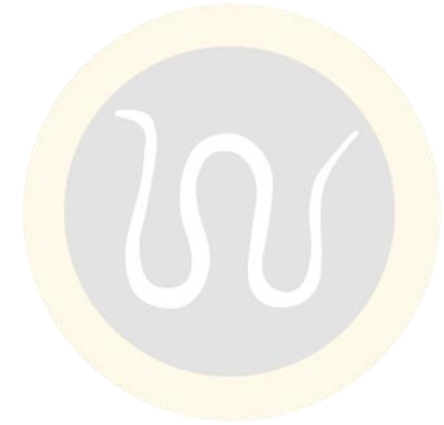
Dario Esposito



Lorena Corna



Sara Martucci



This is an **iason creation**.

The ideas and the model frameworks described in this presentation are the fruit of the intellectual efforts and of the skills of the people working in iason. You may not reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of iason.

www.iasonltd.com