REPLY AVANTAGE

STEPHENSON HARWOOD

From Copilots to Autonomous Agents: Who is Accountable?

To hear more:

Register your interest in the Avantage Reply and Stephenson Harwood event on 25 February 2027, details below.

November 2026

FT FINANCIAL TIMES statista UK'S LEADING MANAGEMENT CONSULTANTS 2026

REPLY AVANTAGE Risk & Compliance TOP CONSULTING FIRM 2026

2027 Chambers Top Ranked UK Stephenson Harwood LLP

Legal500 LEADING FIRM UNITED KINGDOM 2027

Disclaimer from Avantage Reply and Stephenson Harwood

Avantage Reply and Stephenson Harwood have collaborated to prepare this presentation and will be collaborating to deliver the advertised event. This presentation has been prepared for general information and discussion purposes only. It does not constitute legal, regulatory or other professional advice and should not be relied upon as such.

The content reflects the legal and regulatory landscape, guidance and publicly available information as at the date of presentation. Any references to regulatory publications, industry guidance and legal commentary are provided for illustrative purposes and should not be interpreted as establishing additional legal or regulatory obligations.

The application of legal and regulatory requirements and any views expressed in this document to artificial intelligence, including agentic AI, will depend on the specific facts and circumstances. Given the evolving nature of AI technologies and their regulation, organisations should seek appropriate professional advice before making decisions or implementing measures based on the matters discussed.

Whilst reasonable care has been taken in preparing this material, no representation or warranty is given as to its completeness or accuracy. To the extent permitted by law, Avantage Reply and Stephenson Harwood accept no liability for any loss arising from reliance on this presentation.

© 2026 Avantage Reply and Stephenson Harwood. All rights reserved.

AI is moving faster than firms can govern

- AI is evolving from supporting human decisions to independently planning, interacting with systems and executing actions, **creating significant opportunities** for financial institutions while **introducing new risks and amplifying existing ones**.
- **Regulators are increasingly concerned** about the emergence of agentic AI and the implications of greater autonomy for existing regulatory and governance frameworks.
- As AI agents act with less direct human intervention, **traditional lines of responsibility become blurred**, challenging firms' ability to maintain meaningful oversight and demonstrate accountability. However, **firms' legal responsibility has not shifted.**
- Boards and senior management **must ensure operations, governance and accountability keep pace** with emerging technological capabilities.

> **Poorly governed AI can create consumer harm, cyber vulnerabilities and operational failures, potentially at much greater speed and scale.**
>
> — Jessica Rusu, FCA Chief Data, Information and Intelligence Officer[1]

This publication will explore



The opportunities and risks of agentic AI

The value agentic AI can create across financial services and the risks it amplifies *(page 4).*



Why existing frameworks are not enough

Increasing autonomy challenges traditional approaches to governance, risk management and accountability *(page 5-6).*



A way forward

Practical considerations for boards and senior management to strengthen governance, oversight and accountability as agentic AI scales *(page 7).*

[1] FCA Speech, 'Building the future of finance in the age of AI'

Greater autonomy creates opportunity – and amplifies risks

The Opportunities

Regulatory compliance
Monitor regulations, analyse data and draft or file reports.
Greater efficiency and coverage

Customer service and complaints
Handle enquiries, process complaints and issue redress.
Faster, more consistent customer experience

Financial crime and cyber defence
Investigate alerts, triage cases and interact with systems.
Improved detection and reduced costs

Risk management
Monitor exposures, run scenario analyses and trigger risk mitigants.
More timely and data-driven insights

Trading and markets
Analyse market data, execute trades within parameters and manage positions.
Increased speed and market opportunities

Consumer lending
Assess creditworthiness, process applications and support lending.
Faster decision making and improved consistency



The Risks

Operational and Model Risk
Autonomous actions can propagate errors across interconnected systems, disrupting operations.

Conduct Risk
Autonomous decisions can amplify unfair outcomes and customer harm, and potentially breach regulatory obligations.

Cybersecurity and Resilience Risk
Expanded attack pathways, such as prompt injection and privilege misuse.

Reputational Risk
Unintended agent actions and customer harm can undermine institutional trust.

Legal and Regulatory Risk
Autonomous execution complicates demonstrating compliance and determining legal liability.

Financial Risk
Erroneous decisions can trigger rapid, cumulative losses, with corresponding gaps in contractual liability protection and potentially insurance arrangements.

Supply Chain, Third-Party Dependencies and Concentration Risk
Reliance on shared AI models, cloud infrastructure and providers can limit firms' control and create concentrated vulnerabilities. This may expose gaps in contractual liability protections, while unknown AI use in the supply chain could result in a firm's own breaches of contractual or regulatory obligations.

Existing frameworks provide a foundation but need to evolve

Where gaps are emerging



Risk Assessment

Existing risk frameworks may not adequately capture emerging risks arising from autonomous decision-making, multi-step workflows and interactions between agents and external systems.



Governance Frameworks

Traditional oversight may rely on human approval at defined points, creating gaps in decision rights, accountability, escalation and ensuring regulatory compliance as agents act independently.



Controls and Assurance

Model validation and periodic testing may not sufficiently capture dynamic agent behaviour, evolving tool interactions or inappropriate actions executed between monitoring intervals.

FCA supervisory observations[1]

Retrospective governance

Some firms deployed AI before establishing appropriate governance, creating gaps in accountability.

Static monitoring

Some firms relied on point-in-time reviews or technical metrics without sufficient monitoring of outcomes.

Unclear responsibilities

Fragmented ownership and insufficient documentation made it harder to demonstrate effective oversight.

What needs to change

Existing frameworks should be enhanced to address the specific risks and opportunities of agentic AI.

1 | Know your technology stack

Map the AI technology stack, tools and dependencies, to identify vulnerabilities and determine appropriate controls and mitigations.

2 | Strengthen governance

Define accountable owners, autonomy limits, decision rights and escalation arrangements, with regular and ongoing review throughout the agent lifecycle.

3 | Enhance controls and assurance

Introduce scenario-based testing, granular permissions, continuous monitoring and mechanisms to restrict or suspend agent activity.

4 | Demonstrate regulatory compliance

Identify and map AI deployments to applicable obligations, identify control gaps and maintain evidence of effective oversight and assurance.

[1] FCA, AI in financial services: good practice and areas for improvement

Autonomous AI challenges traditional models of accountability

Why agentic AI makes accountability more challenging

Greater autonomy, speed and complexity can make it harder to understand, oversee and attribute responsibility for outcomes.

Speed and scale

Actions can be executed in seconds, across multiple systems and at large scale.

Complexity

Multi-step decisions can involve several agents, tools and third-party systems.

Limited visibility

It can be difficult to trace how decisions were made and to intervene in real time.

Accountability under SMCR and financial regulation

Existing SMCR obligations apply to AI, including agentic AI. Senior managers are not expected to be technical specialists but must take reasonable steps to ensure effective governance, oversight and risk management of AI systems within their areas of responsibility, including for Operational Resilience.

The **FCA identified the following good practices** in the governance and accountability of AI in financial services.[1]

- Assigning clear SMF ownership for AI risks
- Accountability assigned at the beginning of the AI lifecycle
- Informed, documented and auditable SMF oversight
- Clear escalation routes
- Targeted SMF training
- Periodic review of governance arrangements
- Clear ownership of AI agents

Potential liability under English law

AI does not currently have separate legal personality under English law. Existing legal principles therefore govern liability for AI-related harm, potentially exposing financial institutions and AI suppliers depending on the circumstances.

The UK Jurisdiction Taskforce's (UKJT) Legal Statement on Liability for AI Harms[2] confirms this. Liability will depend on the circumstances, including foreseeability and extent of human oversight. Firms may be liable in the following situations, including:

- **Negligence and breach of contract**: firms may be liable where AI (including agentic AI) failures breach a duty of care and cause foreseeable harm, or where they breach contractual obligations, depending on agreed terms. Supplier contracts may exclude AI performance warranties, disclaim liability for underlying models and impose inadequate liability caps, limiting firms' ability to recover losses.
- **Misrepresentation**: for false or misleading AI-generated statements made on their behalf
- **Intellectual property infringement:** where AI models have used third-party IPR unlawfully, and/or client confidential information or personal data
- **Liability**: vicarious liability for employees' actions or omissions and for those of the AI solution

[1] FCA, AI in financial services: good practice and areas for improvement
[2] UK Jurisdiction Taskforce (UKJT) Legal Statement on Liability for AI-related harms

A suggested way forward

The Board Agenda

Key questions for boards and senior management as agentic AI moves from pilots to production:

1 | Strategic Rationale

How does agentic AI support our strategy, risk appetite and customer outcomes?

2 | Key Risks

What are the most material risks and how will they be managed?

3 | Accountabilities

Who is accountable for each AI use case, and how are responsibilities and liabilities allocated internally and with third-party suppliers?

4 | Readiness

Do we have the people, skills, data, infrastructure and culture to adopt safely?

5 | Third-Party Reliance

Do we understand our AI dependencies and have visibility and control over provider use and changes in supply chains?

6 | Legal and Regulatory Compliance

Are we meeting existing obligations and addressing potential liabilities, reviewing and adapting our contracts, and preparing for evolving client and regulatory expectations?

From Principles to Practice

An effective governance framework translates high-level accountability into practical measures across the AI lifecycle.



Define and prioritise

Set clear objectives, risk appetite and use case prioritisation.

- Conduct an AI audit to identify existing use cases, agents, owners and dependencies.
- Align AI use cases with strategy, risk appetite and customer outcomes
- Assess risks across end-to-end agent workflows
- Maintain a central inventory of agents, owners and permissions

Assign and enable

Establish clear accountability and provide the necessary capabilities.

- Allocate clear SMF and operational accountability
- Define decision rights, escalation routes and approvals
- Equip staff and oversight functions with AI-specific skills

Implement and control

Put in place controls proportionate to risk and autonomy.

- Apply risk-based testing and pre-deployment challenges
- Set autonomy limits, human intervention and escalation thresholds
- Test incident playbooks and third-party fallback arrangements
- Review existing AI supplier contracts and ensure future agreements adequately address AI-related risks

Assure and monitor

Provide ongoing independent assurance and transparency.

- Continuously monitor performance, drift and customer outcomes
- Maintain auditable records of decisions and interventions
- Independently review controls and refine them as risks evolve

REPLY AVANTAGE

STEPHENSON HARWOOD

SAVE THE DATE

Click here to register your interest.

From Adoption to Incident: Building AI Resilience in Financial Services

Join Avantage Reply and Stephenson Harwood for a discussion on how financial institutions can build resilience as AI moves from assisting decisions to taking autonomous action.

Date

Thursday, 25 February 2027
18:00 to 21:00

Location

Stephenson Harwood
1 Finsbury Circus
London EC2M 7SH

What to expect

Expert perspectives
Insights from industry leaders, regulators and legal and technology experts.

Practical discussion
Key challenges and real-world considerations for building responsible and resilient AI capabilities.

Actionable takeaways
Practical steps for boards and senior management to strengthen governance, oversight and controls.

Further details, including the agenda and speaker line-up, will be shared soon.

REPLY AVANTAGE

STEPHENSON HARWOOD



Vishwas Khanna
Partner
vi.khanna@reply.com



Marty Clark
Partner
m.clark@reply.com



Kavisha Sharma
Senior Consultant
kav.sharma@reply.com



Esha Pattar
Consultant
e.pattar@reply.com



Simon Bollans
Partner
simon.bollans
@stephensonharwood.com



Christophe Boucherie
Partner
christophe.boucherie
@stephensonharwood.com



Sally Samadi
Partner
sally.samadi
@stephensonharwood.com



Mark Lewis
Senior Consultant
mark.lewis
@stephensonharwood.com

FT FINANCIAL TIMES | UK'S LEADING MANAGEMENT CONSULTANTS 2026
statista

REPLY AVANTAGE Risk & Compliance

TOP CONSULTING FIRM 2026

2027 Chambers Top Ranked UK
Stephenson Harwood LLP

Legal500 LEADING FIRM UNITED KINGDOM 2027

www.reply.com