AI IN FINANCE | AI GOVERNANCE · CYBER RISK · REGULATION · UNITED KINGDOM

United Kingdom regulators set out how firms should handle AI-driven cyber risk: faster patching, AI terms in supplier contracts and board oversight

Published 23 November 2026 · The Finance Intellect · Source-based summary

On 19 November 2026 the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA) and the Bank of England jointly published effective practices on cyber risk relating to AI, with a companion paper on quantum computing. They also opened a consultation on cyber risk and resilience management, PRA CP17/26 and FCA GC26/9, which closes on 26 February 2027.

Global reference

- Country: United Kingdom
- Authorities: Prudential Regulation Authority, Financial Conduct Authority and Bank of England, jointly
- Documents: Effective practices on cyber risk relating to AI; a companion paper on quantum computing; consultation PRA CP17/26 and FCA GC26/9
- Key dates: Published 19 November 2026; consultation closes 26 February 2027
- Status: Effective practices are not formal expectations. The consultation is a draft supervisory statement and FCA guidance

What the AI effective practices say

- Move from periodic vulnerability management to "continuous exposure management".
- Set risk-based remediation targets, with emergency remediation for the most critical vulnerabilities. Treat patching speed and backlogs as operational risks.
- Automatic patching, particularly "hot patching", is "strongly encouraged" where feasible.
- Where a fix cannot be applied, use temporary controls, name an accountable owner and agree a dated remediation plan.
- Scrutinise AI-generated code as well as human-written code, and use phishing-resistant multi-factor authentication against deepfakes.

Suppliers and boards

- Review contracts with material third parties for disclosure of embedded AI, service levels for fixing vulnerabilities and prompt notice of changes to AI systems.
- Document dependencies on open-source and open-weight AI tools, which carry no supplier to turn to.
- Boards should seek assurance on whether controls work, not just how they are designed.

- FCA chief executive Nikhil Rathi: "Our response shouldn't always be more rules."

What to do now

- Ask IT for the current backlog of critical vulnerabilities and the average time to fix, and report it to the audit or risk committee.
- Add AI clauses to supplier contract reviews: embedded AI, fix times and notice of AI changes.
- Make sure AI agents and AI tools appear in user access reviews with least-privilege access.
- If you are regulated in the United Kingdom, plan a response to the consultation before 26 February 2027.

Our take

This is practical guidance, not new rules. Most of it is good hygiene that finance teams can push for even outside the United Kingdom: faster fixes, named owners and clear AI terms with suppliers. The supplier clauses are the easiest win, because procurement and finance already own those contracts.

Sources

- Bank of England: Effective practices: Cyber risk and resilience management relating to artificial intelligence (AI) (19 November 2026)
- Bank of England: Effective practices: Cyber risk and resilience management relating to quantum computing (19 November 2026)
- FCA press release via EuropaWire: FCA and Bank of England propose cyber resilience guidance for UK financial firms as threats intensify (19 November 2026)
- RegReportingDesk: PRA CP17/26 and GC26/9: Cyber Risk and Resilience Guidance (20 November 2026)

Important. This summary is for general information and is not legal, regulatory or technology advice. It is based on public PRA, FCA and Bank of England publications and may be incomplete or out of date. The official publications prevail; check the official source before acting.

ABOUT THE FINANCE INTELLECT

A Finance Knowledge & Resource Platform by Neocor Consultancy. Weekly tax and finance insights, Excel templates, calculators and a learning hub for finance leaders and professionals.

Platform: thefinanceintellect.com | **Owner:** neocorconsultancy.com