Who controls the technology behind a UK mid-size financial firm?

How much a typical mid-size financial firm depends on a handful of technology suppliers it cannot fully control — and where that matters most.

Martin De Saulles | Principal Analyst · June 2026

The big picture

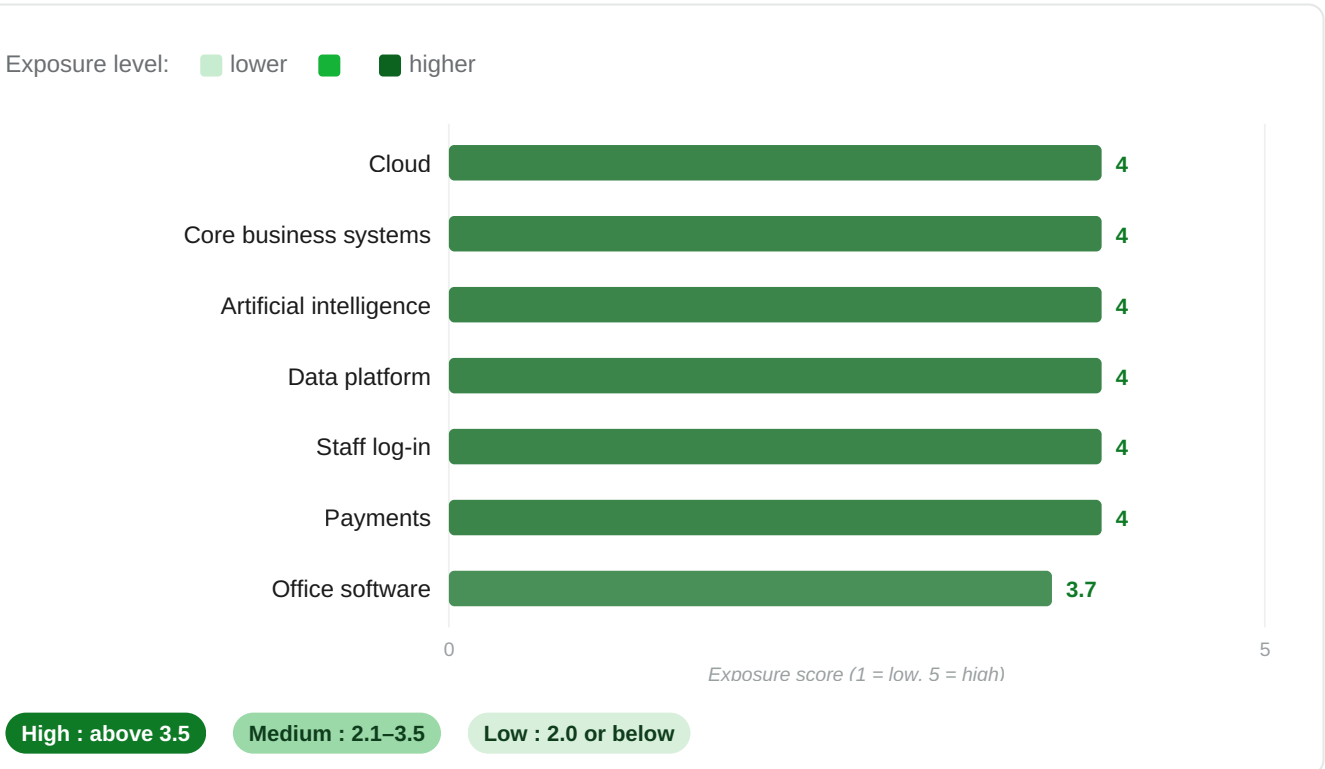
3.6 / 5

HIGH EXPOSURE

A typical UK mid-size financial firm runs on a small number of mostly US-owned technology suppliers — and roughly two-thirds of the most critical parts trace back to a single company, Microsoft. For the most important layers there is no easy way to switch and no home-grown alternative ready to step in. The clearest exception is the firm's own banking, which sits under UK law.

We looked at seven layers of technology the firm relies on and scored each from 1 (low exposure) to 5 (high). The score weighs how few the suppliers are, whose laws they answer to — a US-owned supplier can be compelled to hand over data under the US CLOUD Act even when that data sits in Britain[1] — how hard they are to switch, and how essential they are. UK regulators already treat heavy reliance on a few cloud and AI providers as a risk to the stability of the financial system.[5]

Where the exposure sits



All seven layers fall in the high band — an unusually concentrated picture. The exposure comes less from any one weak spot than from how much depends on the same few US suppliers.

What this means, in plain terms

The cloud is the foundation — and it is American. Almost everything else runs on top of it, and the market is dominated by three US providers (Amazon, Microsoft, Google). A UK region helps, but does not put the data beyond US legal reach.[1]

One company sits under most of the stack. Microsoft directly controls the cloud, the email and documents, the AI and the staff log-in — and once the data platform that runs on its cloud is counted, roughly two-thirds of the critical stack depends on Microsoft alone.[3] If that one supplier were lost, much of the firm could go down together.

The firm's own banking is the bright spot. Unlike a high-street bank's payment rails, a mid-size firm's banking and client accounts sit with UK banks under UK law — the one clearly low-exposure part of the picture.

Artificial intelligence is the cheapest thing to fix. It carries the sharpest confidentiality risk, but open models such as Mistral (France) or Llama can be run on the firm's own infrastructure — among the fastest, cheapest ways to lower exposure.

Core systems have real UK and European choices. Core banking and policy platforms are one layer with genuine non-US options (for example Thought Machine, Temenos, Mambu, SAP),[4] so the firm is not locked in here — the decision point is the next contract renewal.

If a supplier pulled the plug, how fast would it hurt?

SPEED OF IMPACT	LAYER	WHAT HAPPENS
Immediate	Staff log-in	Staff locked out across all systems at once, with no warning.
Within days	Cloud · Data platform	Services running on the cloud degrade; analytics and reporting stop.
Weeks	Artificial intelligence	Easiest to replace — alternatives and open models can fill in.
Weeks–months	Core systems · Office	Contracts and exported data give some breathing room to move.
Months+	Payments	Card-scheme disruption would bite, but the firm's UK banking keeps working.

What firms can do about this

BUILDING BLOCK	PRACTICAL STEPS
Artificial intelligence	Run an open model the firm controls (for example Mistral or Llama) on UK or European hosting for sensitive work — the quickest, cheapest win.
Cloud	Hold your own encryption keys; keep a tested copy of critical systems in a UK/EU sovereign region or with a second provider (for example the AWS European Sovereign Cloud[6]); write exit and data-portability rights into every contract.
Core systems	Favour a UK or European platform at the next renewal (for example Thought Machine, Temenos, Mambu or SAP[4]); write data-portability and exit-assistance clauses in.
Staff log-in	Keep a rehearsed fallback for signing in — emergency admin access and a back-up identity provider. The open-source system Keycloak, self-hosted, reduces reliance on a single US provider.
Data platform	Keep data in a UK/EU region, hold your own keys, and favour open table formats (such as Apache Iceberg) so the data is not trapped in one vendor's system.
Payments	Use domestic UK rails (Faster Payments, Bacs, run by Pay.UK) where the use-case allows, rather than the international card schemes.

Sources

1. US CLOUD Act 2018 (18 U.S.C. §2713) — compels US-incorporated providers to produce data in their custody wherever stored. https://www.congress.gov/bill/115th-congress/house-bill/4943
2. US Foreign Intelligence Surveillance Act, Section 702 (50 U.S.C. §1881a) — directed-surveillance authority. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section1881a
3. Microsoft, Salesforce, Snowflake, Visa and Mastercard — controlling-entity domicile from annual reports (Form 10-K), via SEC EDGAR. https://www.sec.gov/edgar
4. Thought Machine Group Ltd — UK incorporation and ownership, Companies House. https://find-and-update.company-information.service.gov.uk/company/11114277
5. Bank of England & FCA — *Artificial intelligence in UK financial services* survey (2024) and the Critical Third Parties regime (PS24/16, in force January 2025). https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024
6. Amazon Web Services — *Opening the AWS European Sovereign Cloud* (15 January 2026). https://aws.amazon.com/blogs/aws/opening-the-aws-european-sovereign-cloud/

How we did this. We scored seven technology layers on four things — how concentrated the suppliers are, whose laws they answer to, how hard they are to switch, and how essential they are. Control and ownership facts come from the primary sources listed above; the harder-to-quantify judgments are our reasoned view of a typical firm. Scores are bands, not exact measurements. Full evidence record available on request.

Information Matters · informationmatters.net