INFORMATION MATTERS · DIGITAL SOVEREIGNTY

Who controls the technology behind a UK law firm?

How much a typical mid-size law firm depends on technology suppliers it cannot fully control — and why privileged client files are the part that matters most.

Martin De Saulles | Principal Analyst · June 2026

The big picture

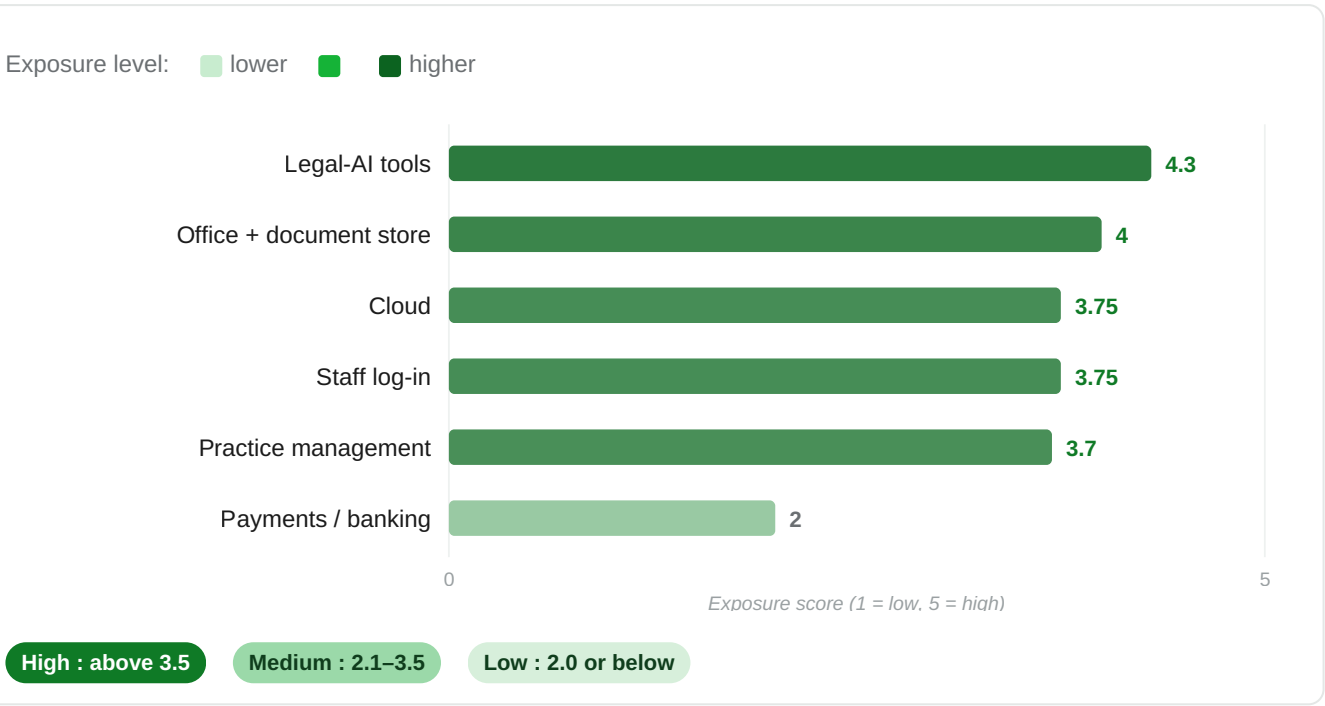
3.6 / 5

HIGH EXPOSURE

A law firm's most valuable and most confidential asset is its client work — privileged advice and decades of case files. For a typical UK mid-size firm, that material lives with mostly US-controlled suppliers, reachable under US law. The one clear exception is the firm's own banking, which sits under UK law.

We looked at six 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 under the US CLOUD Act even when data sits in Britain,[1] which for a law firm touches legal professional privilege and the firm's duties to the Solicitors Regulation Authority[6] — how hard they are to switch, and how essential they are.

Where the exposure sits



Five of the six layers fall in the high band, clustered around one thing: the firm's privileged documents sit with US-controlled suppliers. Payments and banking — under UK law — are the clear exception.

What this means, in plain terms

Privileged files are the defining risk. The firm's lifeblood — privileged work product and decades of matter files — lives in Microsoft 365 and a US document-management system (iManage or NetDocuments), all US-controlled and reachable under US law.[1] It is also the hardest thing to move.

The diversification is often an illusion. The leading document system, iManage, itself runs on Microsoft Azure[3] — so a firm on Microsoft 365 with iManage has its documents, email, log-in and computers all tracing back to one company, Microsoft. The off-Microsoft route is NetDocuments (own data centres plus Amazon).[4]

Legal-AI carries the sharpest confidentiality risk. AI assistants such as Harvey send privileged client content through a US-controlled, closed system[5] — the most sensitive layer, but also the cheapest and fastest to make safer.

Payments is the discriminator. Unlike a bank, a law firm's payments and banking sit with UK banks under UK law — low-exposure, and the clearest contrast with financial services.

The newest layer is the most fixable. For privileged work, open models the firm runs itself keep the material in-house — the quickest win on this list.

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

SPEED OF IMPACT	LAYER	WHAT HAPPENS
Immediate	Staff log-in	Everyone locked out across all systems at once.
Within days	Cloud	Services running on the cloud degrade; email and documents stop.
Weeks	Legal-AI · Practice management	AI is the easiest to replace; billing has some runway.
Months+	Office + document store	The deepest problem — moving decades of privileged files off a US system could take well over a year.
Low risk	Payments / banking	UK banking keeps working — not a crisis layer for a law firm.

What firms can do about this

BUILDING BLOCK	PRACTICAL STEPS

Document store	Be able to export matter files in open formats, and prefer a system that keeps files in the UK or off Microsoft's infrastructure. iManage runs on Microsoft Azure; NetDocuments runs its own data centres plus Amazon — a real choice for a firm avoiding single-supplier concentration.
Legal-AI	Prefer tools you can run privately or that are UK-controlled (for example Luminance, Robin AI, Genie AI, Definely); for the most sensitive work, run open models such as Mistral or Llama on the firm's own infrastructure.
Cloud & log-in	Reduce the Microsoft concentration by moving the cloud and/or staff log-in to another supplier — UK/European options include OVHcloud, Scaleway, IONOS and Civo; the open-source system Keycloak, self-hosted, reduces reliance on a single US provider.
Practice management	Prefer a UK-controlled supplier at renewal — UK-built options include Osprey Approach, Insight Legal, Linetime and Peppermint.
Payments / banking	Already low-risk — accept and monitor.

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). https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section1881a
3. iManage — Trust Center: iManage Work runs on Microsoft Azure, with a UK data region. https://imanage.com/about/trust/
4. NetDocuments — Trust Center: own hybrid-private cloud plus Amazon Web Services; UK login region. https://www.netdocuments.com/trust
5. Harvey — platform agreement and privacy policy (Harvey AI Corporation, a Delaware corporation). https://www.harvey.ai/. Microsoft / Aderant (Roper Technologies) / Okta domicile via SEC EDGAR. https://www.sec.gov/edgar
6. Solicitors Regulation Authority — Standards and Regulations (confidentiality and outsourcing duties). https://www.sra.org.uk/solicitors/standards-regulations/

How we did this. We scored six 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, ownership and hosting 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