Daniel Young Advisory
FRACTIONAL CIO · CYBERSECURITY · AI GOVERNANCE · DUBAI, UAE

daniel@danielpyoung.com
danielpyoung.com
+971 58 563 9178

CASE STUDY · AI GOVERNANCE

From uncontrolled experimentation to board-approved AI adoption

9	7	≈6,953	380
AI TOOLS FORMALLY APPROVED	TOOLS REVIEWED AND BLOCKED	AI ACCESS ATTEMPTS BLOCKED PER MONTH VIA DNS	STAFF COVERED BY POLICY AND TRAINING

THE CHALLENGE

When AI adoption precedes governance

At an FCA-regulated wealth manager with 380 staff and 11 UK locations, AI adoption had reached the business before any governance was in place. Staff were using tools informally across research, client communications, software development, and workflow support. No policy existed, and no data classification defined what could enter a public AI tool.

There was no approval workflow, no named owner, and no visibility over which tools were in active use or what data was being shared. The firm faced latent exposure to client data leakage and regulatory breach. Internal views were split between full restriction and unrestricted use, with no senior technology owner to establish a defensible position.

A frequently overlooked dimension: existing third-party suppliers were beginning to embed AI into services involving client data transfer, with no framework to assess their governance. The same pattern is common across DFSA- and FSRA-regulated firms now navigating GenAI adoption without governance in place.

THE RESULT

A board-approved, defensible governance position that enabled controlled adoption

The firm moved from uncontrolled AI use to a governance position approved at board level by the Audit & Risk Committee. Nine tools were formally whitelisted from a default-ban position; seven reviewed tools were blocked - more than 40% of tools assessed.

Nearly 7,000 AI access attempts were blocked per month via DNS enforcement - providing measurable evidence of active enforcement. Shadow AI curtailed through default-ban design: staff had a route to request tools rather than simply bypass controls.

Client disclosure was embedded in Terms & Conditions. Third-party AI risk was integrated into the supplier lifecycle - DeepSeek was blocked on data sovereignty grounds under the framework. The board could evidence the firm's AI position to regulators and clients.

THE PROGRAMME

Governance is not a policy document in SharePoint - it is a board-owned, enforceable framework the business can operate within and the regulator can scrutinise

POLICY & DATA CLASSIFICATION
Co-authored inaugural AI Acceptable Use Policy, approved at Audit & Risk Committee. Data classification defined which data classes cannot enter public AI tools, aligned to FCA obligations and UK GDPR.

DEFAULT-BAN / WHITELIST
All AI tools prohibited until formally assessed and whitelisted centrally through the IT Operations team. Staff had a defined route to request tools; the default position was documented and enforced.

AUTHORISATION WORKFLOW
Structured AI Sponsor Form requiring a named business sponsor, data sovereignty check, confirmation of model training opt-out, and mandatory sign-off by IT Director, COO, and Chief Transformation Officer.

AI REGISTER
Live register of all approved tools with named owners, risk classifications, approved use cases, and scheduled review dates - maintained as an active governance record, not a static inventory.

SUPPLIER GOVERNANCE
Worked with Risk and Outsourcing teams to embed AI governance checks into supplier onboarding and annual review - covering data handling, security certifications, IP ownership, model training rights, and AI embedded in client-data-related services.

DNS ENFORCEMENT
DNS-level detection and blocking of non-approved AI tools across 117M+ monthly queries. Provided measurable evidence of active enforcement across all 380 staff - not policy on paper alone.

A default-ban position is only effective if the approval pathway is accessible - staff will route around controls that create more friction than bypassing them. The supplier dimension is equally critical: third parties embedding AI into client-data services represent an exposure the internal framework cannot see and does not address.

DFSA & FSRA RELEVANCE

The FCA's principles-based approach to AI governance - transparency, human-in-the-loop validation, consumer duty obligations, and third-party oversight - maps directly to regulatory expectations under the DFSA and FSRA. Firms in DIFC and ADGM experimenting with GenAI without a documented framework face the same exposure: shadow AI use, undefined data boundaries, and an inability to evidence their approach under regulatory scrutiny. The governance architecture here - policy, classification, authorisation workflow, register, and supplier checks - is directly applicable to the UAE regulatory context.

DIFC & ADGM-REGULATED FIRMS

The gap between informal AI experimentation and board-owned governance is a live compliance exposure. Regulated firms require a documented governance position before a regulatory event.

- Define a governance position: policy, data classification, and a default-ban/whitelist that staff will use rather than bypass.
- Build an authorisation workflow that is faster than going around it - so approved adoption accelerates rather than stalls.
- Embed AI governance into the supplier lifecycle before the next contract renewal or regulatory review.

Engagements typically start with an AI governance diagnostic: reviewing current tool usage, mapping unmanaged exposure, and producing a board-ready framework, acceptable use policy, and remediation roadmap.