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

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

CASE STUDY · CYBER MATURITY

Building a realistic cyber maturity programme at a regulated wealth manager - and what it means for DIFC and ADGM firms

50%	40%	10+	ISO
REDUCTION IN PHISHING INCIDENTS	IMPROVEMENT IN INCIDENT RESPONSE TIME	YEARS OF CLEAN REGULATED AUDIT RECORD	27001-ALIGNED CONTROLS THROUGHOUT

THE CHALLENGE

When 'good enough' stops being enough

The gap between having security controls and demonstrating a defensible security posture is where most regulated firms get caught. The problem is rarely a lack of investment - it is a lack of sequence.

At Killik & Co, an FCA-regulated wealth manager operating across 11 UK locations, cyber maturity became a board-level priority not because of a major breach, but because the regulator, insurers, and clients all started asking the same question at once: "show us your controls".

Point-solutions and historic projects could not be explained as a coherent security posture the board could own.

THE RESULT

From ad-hoc controls to a defensible posture

Phishing incidents fell by 50%, and incident response times improved by 40% under the new operating model. The firm maintained a clean FCA-regulated audit record throughout and could take a documented, defensible position with both the board and the regulator on its security posture.

The success factor was not any single control. It was treating cyber maturity as a structured programme with sequenced decisions, clear ownership, and evidence - rather than a series of disconnected security projects.

THE PROGRAMME

Leading the IT function also meant wearing the CISO hat and designing a realistic programme the firm could sustain

MFA & IDENTITY CONTROLS
Multi-factor authentication across all users and critical systems. Reduced credential risk and formed the basis of a more identity-centric security model.

24/7 MANAGED SOC
Defined what "monitoring" meant in practice: alert triage, escalation paths, and response expectations - not just a log aggregation service.

STAFF AWARENESS
Continuous campaigns, measurement, and targeted follow-up for high-risk users, rather than once-a-year training.

POLICY FRAMEWORK
Clear, enforced policies tied to real controls and refreshed on a fixed cadence.

LEGACY REMOVAL & ACCREDITATION
Retired unsupported platforms and aligned to ISO 27001-style controls, using Cyber Essentials as the baseline accreditation, with the environment prepared for Cyber Essentials Plus.

PRIVILEGED ACCESS REVIEW
PAM requirements formally scoped and assessed. Implementation sequenced as the next maturity step; environment structured to support deployment without service disruption.

Each step was prioritised and justified in terms of audit findings, insurance requirements, and regulatory expectations, so the board could see why it mattered and what changed.

AI & CYBER RISK

The controls that underpin cyber maturity - identity management, data classification, policy governance, SOC oversight - are the same foundations required to govern AI adoption safely. Generative AI tools expand the attack surface through OAuth integrations, data ingestion pipelines, and shadow usage across the business. Firms that have not resolved their cyber posture have no reliable basis for governing AI at board level. Building cyber maturity and AI governance in parallel is the defensible approach for DFSA and FSRA-regulated firms.

DIFC & ADGM-REGULATED FIRMS

DFSA- and FSRA-regulated firms in DIFC and ADGM are at the same inflection point: regulatory scrutiny, insurer pressure, and client due diligence on cyber controls are converging.

- Establish a clear baseline and control roadmap.
- Sequence MFA, SOC, awareness, policy, and legacy system removal.
- Align to recognised frameworks and produce board-ready evidence of posture and gaps.

> *Engagements typically start with a focused cyber posture review: controls, incidents, supplier coverage, and a board-ready view of strengths, gaps, and quick wins.*