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

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

TECHNOLOGY RISK REVIEW · FIXED-FEE CYBERSECURITY DIAGNOSTIC

A board-ready assessment of your cybersecurity posture - control gaps, SOC readiness, and a prioritised remediation path, delivered in three weeks

AED 28,000	3-4 days	2-3 wks	1
FIXED FEE, NO DAY-RATE BILLING	ON-SITE ASSESSMENT AND REVIEW	ENGAGEMENT TO DELIVERY	WRITTEN REPORT, BOARD-READY

THE PROBLEM

Most boards can't see their actual cyber exposure

Cybersecurity is now a standing board agenda item at regulated firms, but most boards are working from vendor assurances and incident-free history rather than an independent view of where the gaps actually are.

DFSA and FSRA expectations are explicit: firms must maintain a documented cyber risk framework, demonstrate control effectiveness, and notify the regulator within a fixed window of any material incident. None of that is possible without first knowing, in writing, where the firm actually stands.

THE OUTCOME

A clear, prioritised, board-usable answer

A structured, independent review of the firm's security posture - control by control - producing a single written report the board or compliance committee can act on directly.

Findings are risk-rated and sequenced, so the immediate question - what needs fixing first, and what it will take - has a documented answer rather than a verbal assurance.

WHAT'S REVIEWED

A focused review across the areas that matter most to the regulator and the board

CONTROL ENVIRONMENT
Policies, ownership, and governance structure assessed against ISO 27001 and NIST CSF.

IDENTITY & ACCESS
MFA coverage, privileged access management, and access review discipline.

INCIDENT RESPONSE
SOC readiness, detection capability, escalation paths, and response plan maturity.

DATA & THIRD-PARTY EXPOSURE
Data classification discipline and security obligations across key supplier relationships.

HUMAN RISK
Phishing exposure, awareness training coverage, and behavioural control gaps.

REGULATORY MAPPING
Findings mapped directly to DFSA cyber risk expectations - strategy, governance, monitoring, response.

Each finding is risk-rated and sequenced into a single remediation roadmap - not a checklist, a prioritised plan the board can approve and track.

SCOPE & BOUNDARIES

This is a control and governance review, not a penetration test and not a certification audit - it will not produce an ISO 27001 certificate or a technical exploit report. It also does not cover operational resilience (service mapping, RTO/RPO, business continuity) or AI governance (acceptable use policy, generative AI risk) - those are separate, scoped engagements available once this review identifies where they're needed. Findings are informed by ISO 27001 and NIST CSF and mapped to DFSA expectations; this is an independent assessment, not a certification assurance. Where a control or policy is absent, it will be identified, risk-rated, and prioritised for remediation - full drafting or implementation is out of scope unless separately commissioned.

DIFC & ADGM-REGULATED FIRMS

DFSA- and FSRA-regulated firms are expected to maintain a documented, board-approved cyber risk framework, demonstrate ongoing control effectiveness, and notify the regulator of material incidents within a fixed window. A Technology Risk Review gives the board the documented baseline that framework depends on.

- Assess the control environment against ISO 27001 and NIST CSF, informed by FCA-regulated practice.
- Identify and risk-rate gaps in identity, access, incident response, and supplier exposure.
- Map findings directly to DFSA cyber risk expectations for board and compliance committee use.
- Deliver a single, prioritised remediation roadmap - not a list of issues without a plan.

Built from twenty years operating inside an FCA-regulated cyber risk framework, applied directly to the DFSA and FSRA control environment.

> *Engagements begin with a short scoping call to confirm fit, followed by structured interviews and control review over three to four days, with the written report delivered within two to three weeks. Fixed fee, agreed before the work begins.*