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

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

OPERATIONAL RESILIENCE BASELINE · FIXED-FEE RESILIENCE DIAGNOSTIC

A board-ready view of your operational resilience posture against the DFSA's proposed operational resilience framework: critical business services, impact-tolerance questions, and dependency gaps

AED 28,000	4-5 days	Up to 4 wks	1
FIXED FEE, AGREED BEFORE WORK BEGINS	STRUCTURED INTERVIEWS AND EVIDENCE REVIEW	KICK-OFF TO BOARD REPORT	WRITTEN REPORT, BOARD-READY

THE PROBLEM

Continuity plans describe recovery. The board needs to understand the service.

Most regulated firms have some form of IT continuity documentation. Fewer have a board-owned account of which business services clients and regulators rely upon, how much disruption each service can tolerate before harm becomes unacceptable, and what evidence supports that view.

DFSA's proposed direction places greater emphasis on the continuity of critical business services, building on existing business continuity and crisis management arrangements. It points firms towards identifying critical services, defining impact tolerances, mapping dependencies, testing severe but plausible disruption, and maintaining evidence throughout.

For firms without a dedicated technology or resilience function, the gap is often invisible until a board challenge, regulatory conversation, or live incident exposes it.

THE OUTCOME

A documented baseline, not a generic maturity score.

An independent assessment producing one board-usable written report. It provides a draft inventory of critical business services, a high-level view of the people, technology, data, premises, and external services those services rely on, and preliminary impact-tolerance questions for board decision, compared against stated recovery capability and available evidence.

The report also provides a gap assessment mapped to the DFSA's proposed framework and a prioritised remediation roadmap, sequenced by regulatory and operational risk - distinguishing what the firm can already evidence from what a full service-mapping engagement would need to establish.

Deliverable: typically a 12 to 18-page board report - a maturity view across six modules, draft critical-service inventory, dependency observations, risk-rated findings, and a prioritised 90-day / 12-month roadmap.

WHAT'S REVIEWED

Six review modules, mapped directly to DFSA's proposed framework

CRITICAL BUSINESS SERVICES
Draft identification of the services whose disruption could materially harm clients, counterparties, or the firm's ability to meet regulated obligations.

SERVICE DEPENDENCY MAPPING: LITE
High-level identification of stated dependencies across people, technology, data, premises, and material outsourced or group-provided services.

IMPACT TOLERANCE QUESTIONS
Preliminary business-led thresholds for disruption, and the gap between stated recovery capability and the evidence required for board approval.

SCENARIO & EVIDENCE QUALITY
Whether current plans, tests, and incident evidence address severe but plausible disruption scenarios.

GOVERNANCE & OWNERSHIP
Whether resilience has an accountable executive owner, board oversight, decision rights, and a defined reporting cadence.

REGULATORY GAP MAPPING
Findings mapped to the DFSA's proposed operational resilience direction of travel for DIFC firms, or to the FSRA's existing risk management framework and operational resilience priorities for ADGM firms.

Each finding is risk-rated and sequenced into a single prioritised roadmap - a baseline the board can act on, not a checklist.

SCOPE & BOUNDARIES

A maturity baseline, not a resilience implementation programme. This engagement does not produce:

- A complete or validated end-to-end service map
- Formal board-approved impact tolerances
- Validated recovery objectives or technology recovery commitments
- Tested incident or crisis playbooks
- Supplier resilience due diligence or contractual continuity review
- A cybersecurity control review - covered separately under the Technology Risk Review

Dependencies are identified, not validated. Supplier capability, contractual commitments, and continuity arrangements are assessed only under separately scoped work.

Where the review identifies material gaps, next steps are typically one of: a separately scoped remediation project, policy or documentation drafting, or an ongoing fractional advisory retainer for firms that want continuity of ownership through implementation.

DIFC & ADGM-REGULATED FIRMS

The direction of travel makes operational resilience a business and board issue, not an IT continuity exercise. DIFC firms face the DFSA's proposed operational resilience framework directly; ADGM firms are assessed against the FSRA's existing risk management and cyber risk requirements, with operational resilience flagged as a supervisory priority ahead of a discrete rulebook chapter. Both are proportionate and risk-based, but the central questions are the same: which business services are critical, how much disruption can they tolerate, what do they rely on, and can the firm demonstrate it can remain within those limits?

- Identify critical business services and frame the impact-tolerance decisions requiring board ownership.
- Assess stated recovery capability against preliminary disruption thresholds and available evidence.
- Map gaps directly to the DFSA's direction of travel, or the FSRA's existing risk management framework for ADGM firms.
- Produce a single, prioritised roadmap into full mapping and remediation.

Engagements begin with a short scoping call to confirm fit, followed by structured stakeholder interviews and evidence review over four to five working days. The written report is delivered within up to four weeks. AED 28,000 fixed fee, agreed before the work begins.

Scope assumes one regulated legal entity, up to six stakeholder interviews, review of available documentation, and an initial assessment of up to five critical business services. Additional entities, services, workshops, or supplier reviews are separately scoped.