Daniel Young Advisory

DFSA CYBER RESILIENCE CHECKLIST FOR GCC FIRMS

10 board-level questions every regulated firm should be able to answer in 2026

Firms with three or more governance gaps face elevated thematic review risk. This checklist identifies them in under 20 minutes.

A diagnostic for CIOs, CISOs, COOs and Board Risk / Audit Committees operating under the DFSA, FSRA and related GCC regulatory frameworks.

Published	Author	Distribution
1.1 - March 2026	Daniel Young Advisory	Free resource - distribute with attribution

Working with regulated firms across Dubai and the GCC on technology risk and cyber resilience.
Enquiries: danielpyoung.com

How To Use This Guide

Purpose

This checklist is a diagnostic, not a compliance programme. It is designed to help boards, risk committees and senior executives in regulated GCC financial services firms rapidly identify governance gaps in their cyber risk posture relative to DFSA expectations and the wider regional regulatory environment.

Each of the ten questions identifies a specific regulatory obligation, describes the most common failure modes observed in practice, defines what a defensible position looks like, provides risk signals to watch for, and concludes with a single actionable next step.

Audience	CIOs, CISOs, COOs, Board members, Risk and Audit Committee members.
Regulatory basis	DFSA GEN Module Cyber Risk Management Rules (effective January 2024); FSRA CRMF (effective January 2026); UAE NCA; CBUAE guidance; FCA SYSC; DORA (secondary).
What this is	A governance diagnostic and board-level oversight tool.
What this is not	A vendor selection guide, implementation plan, technical configuration reference or legal advice.
Recommended use	Review quarterly at risk committee level. Use as a pre-thematic review preparation tool. Adapt for board induction programmes.
Reading time	Approximately 20 minutes for individual review; 30 minutes as a structured risk committee agenda item.
Share this	If useful, forward to your risk committee, compliance lead or board secretary.

Self-Assessment Summary

Quick-Reference Board Scorecard

Use the table below to record the firm's current status against each question. Status should be determined by compliance or risk, not by IT. Any 'No' or 'Partial' response represents a governance gap requiring a documented remediation plan.

Not all gaps carry equal regulatory exposure. Questions 1, 4, 5 and 6 represent the areas of highest supervisory risk based on DFSA thematic review findings and the materiality of the obligations involved. A 'No' or 'Partial' response to any of these four should be treated as a priority remediation item regardless of the overall score.

#	Question	Status (Yes / Partial / No)	Owner	Target Date
1	Does the board formally own the cyber risk management framework?			
2	Can the board articulate the firm's cyber risk appetite in quantified terms?			
3	Is the firm's ICT asset inventory current, complete and governing-body accessible?			
4	Has the firm tested its cyber incident response plan in the last 12 months?			
5	Does the firm meet the DFSA's 72-hour material incident notification requirement?			
6	Are third-party and outsourced ICT risks actively governed, not just contractually managed?			
7	Is the firm's cyber resilience testing programme proportionate and independently evidenced?			
8	Does the board receive meaningful, structured cyber risk reporting on a regular cadence?			
9	Is mandatory cyber awareness training completed annually by all staff, including the board?			
10	Has the firm assessed its cyber obligations across all applicable regulatory jurisdictions?			

Firms identifying three or more 'No' or 'Partial' responses should treat this as a priority governance action before the next regulatory contact, thematic review or board risk committee meeting. Any single 'No' against Questions 1, 4, 5 or 6 warrants immediate escalation regardless of total score.

Regulatory Context

The GCC Regulatory Landscape in 2026

The UAE financial services regulatory environment is not monolithic. Firms operating across DIFC and ADGM are subject to materially different cyber obligations under the DFSA and FSRA respectively. The DFSA's rules have been in force since January 2024. The FSRA's more prescriptive CRMF came into effect in January 2026, introducing mandatory ICT contract provisions and a tighter 24-hour incident notification window.

Onshore UAE firms regulated by CBUAE and the UAE NCA Cybersecurity Framework operate under separate but complementary requirements. Firms with European client books or EU-entity relationships must also consider DORA obligations, which are significantly more prescriptive than UAE frameworks in areas such as ICT third-party risk and resilience testing.

Key Regulatory Differences at a Glance

Obligation	DFSA (DIFC)	FSRA (ADGM) from Jan 2026	DORA (EU-nexus)
Incident notification	72 hours (material incidents)	24 hours (material incidents)	4 hours initial; 24 hours detail
Framework approval	Board approval required; written CRMF	Board approval required; written CRMF	Management body approval; prescriptive
Third-party contracts	Governance expected; audit rights	Mandatory contractual provisions	Prescriptive ICT contract requirements
Resilience testing	Comprehensive programme required	Testing obligation in CRMF	TLPT required for significant firms
Asset inventory	Mandatory; current and maintained	Mandatory; current and maintained	Full ICT asset register obligation
Annual staff training	Mandatory; all personnel	Mandatory; all personnel	ICT risk training; awareness programmes
Regulatory stance	Principles-based; thematic reviews	Principles-based; inspection regime	Prescriptive; detailed technical standards

Note: CBUAE and UAE NCA requirements apply to onshore-licensed firms. SCA obligations apply to capital-markets activities. FCA SYSC applies where UK client relationships or authorised entities exist. None of these regimes is fully interchangeable with another.

Q01 Does the board formally own the cyber risk management framework?

Context

DFSA GEN Rule 3.3.31 requires the governing body to approve and maintain a written Cyber Risk Management Framework (CRMF). This is not a delegable technicality. The DFSA 2024 Thematic Review explicitly identified board-level accountability gaps as a primary finding. Regulators assess whether senior management are aware of their firm's cyber vulnerabilities and are providing necessary resources, controls and oversight.

What breaks in practice

- The CRMF exists as a policy document but has never been formally approved by the board.
- Cyber risk is treated as an IT matter: delegated to the CTO or outsourced CISO with no board line of sight.
- Framework is approved once and not reviewed; it becomes a static artefact rather than a living governance instrument.

What good looks like

Board approval	CRMF approved at board or risk committee level, with minutes evidencing the decision.
Annual review	Framework reviewed at least annually and following any material incident or structural change.
Named ownership	A named senior executive (SEO or equivalent) holds accountability, not a committee or team.

RISK: Board cannot describe the firm's current cyber risk posture without referencing an IT briefing note.

RISK: Last board discussion of cyber risk pre-dates 12 months.

RISK: No board resolution or minute evidence CRMF approval.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN 3.3.31 / GEN 3.5.2(1) | FSRA CRMF (effective Jan 2026): mandatory board ownership.	Supervisory finding of inadequate governance; personal accountability risk for SEO under DFSA fitness and propriety rules.

PRACTICAL NEXT STEP
Pull the most recent board or risk committee minutes. Confirm a specific resolution approving the CRMF is recorded. If absent, table it at the next scheduled meeting and document the outcome.

Q02 Can the board articulate the firm's cyber risk appetite in quantified terms?

Context

Risk appetite for cyber cannot remain qualitative. Statements such as 'low tolerance for cyber incidents' have no operational meaning. The DFSA expects firms to integrate cyber risk into their enterprise risk framework, which requires thresholds, escalation triggers and reporting metrics that the board has explicitly set and can defend to the regulator.

What breaks in practice

- Risk appetite is expressed in generic language copied from a framework template.
- No defined threshold for what constitutes a material incident requiring board escalation.
- IT and risk teams use different definitions of materiality, creating reporting gaps.

What good looks like

Quantified thresholds	Maximum acceptable downtime, data loss tolerance, and recovery time objectives are board-approved.
Escalation matrix	Clear trigger points for what requires board notification vs. executive-only response.
Integrated RAS	Cyber risk appetite sits within the firm's Risk Appetite Statement alongside credit, market and operational risk.

RISK: Board members cannot state the firm's recovery time objective (RTO) for critical systems.

RISK: Cyber risk is absent from the firm's Risk Appetite Statement.

RISK: No escalation protocol differentiates board-level from executive-level incidents.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN 3.3.31 | UAE NCA Cybersecurity Framework: risk tolerance integration | CBUAE Operational Risk guidance.	In a supervisory review, inability to demonstrate a calibrated risk appetite signals immature governance and invites closer scrutiny.

PRACTICAL NEXT STEP

Request the current Risk Appetite Statement. Verify that cyber risk thresholds are explicitly included, quantified and board-approved. If absent, commission a one-page addendum for the next board cycle.

Q03 Is the firm's ICT asset inventory current, complete and governing-body accessible?

Context

The DFSA mandates that firms identify and maintain a current inventory of ICT assets. This is not an IT hygiene task; it is the foundation of every other control. You cannot assess risk, manage third-party dependencies, or respond to an incident if you do not know what you own, what it connects to, and what it processes. The 2024 Thematic Review flagged incomplete asset inventories as a persistent gap.

What breaks in practice

- Asset inventory maintained by IT but not reviewed or validated by compliance or risk.
- Cloud services, SaaS subscriptions and shadow IT absent from the register.
- No mapping between assets and the data classifications they process.

What good looks like

Maintained register	Documented, version-controlled ICT asset inventory reviewed at least annually.
Data classification linkage	Assets tagged to data sensitivity levels and regulatory classification.
Board summary view	The risk committee receives a periodic summary of critical asset exposure, not a raw IT list.

RISK: IT team cannot confirm the complete list of third-party services in use across all business lines.

RISK: Asset inventory was last reviewed more than 12 months ago.

RISK: Critical business processes cannot be mapped to their underlying ICT dependencies.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN 3.3.31 | FSRA CRMF: ICT asset identification as mandatory control element.	Incomplete inventories are a direct control gap and a supervisory finding risk during thematic reviews. Incident response becomes guesswork.

PRACTICAL NEXT STEP
Ask the CTO or IT lead to present the current ICT asset register to the risk committee, including cloud services. Identify any gaps between the register and known business systems within 30 days.

Q04 Has the firm tested its cyber incident response plan in the last 12 months?

Context

The DFSA requires firms to maintain a written Cyber Incident Response Plan (CIRP) reviewed at least annually. Review means tested, not just read. The DFSA's supervisory framework includes engagement in cyber simulations and expects firms to have pre-approved communications templates for the most likely incident scenarios. An untested CIRP is not a control; it is a document.

What breaks in practice

- CIRP exists but has never been exercised in a tabletop simulation or live drill.
- Communications templates are generic and not pre-approved by legal, compliance and senior management.
- The post-incident review process is absent; lessons from prior events are not incorporated.

What good looks like

Annual testing	Tabletop exercise or simulation conducted at least annually, results documented.
Pre-approved comms	Templates for regulatory notification, client communication and media response are drafted and signed off.
Lessons learned	Post-exercise findings fed back into the CRMF and CIRP within a defined timeframe.

RISK: No tabletop exercise has been conducted in the past 12 months.

RISK: Incident response roles are assigned to individuals who have not participated in any simulation.

RISK: Pre-approved communications templates for a ransomware scenario do not exist.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN 3.3.31 (CIRP annual review) | DFSA Cyber Supervision Framework: simulation engagement | FSRA CRMF: tested response and recovery obligation.	Without tested procedures, the 72-hour notification obligation to the DFSA becomes operationally undeliverable under pressure.

PRACTICAL NEXT STEP
Confirm the date of the last CIRP exercise. If more than 12 months ago, schedule a tabletop within 60 days. Engage compliance and legal in the exercise design to validate notification procedures.

Q05 Does the firm meet the DFSA's 72-hour material incident notification requirement?

Context

DFSA-regulated firms must notify the DFSA no later than 72 hours after becoming aware that a material cyber incident has occurred, using the prescribed form on the DFSA ePortal. The FSRA (ADGM) has an even tighter window: 24 hours. Materiality encompasses operational, financial and reputational impact. For firms with dual-regulated or cross-border operations, multiple simultaneous notification obligations may apply.

What breaks in practice

- No defined internal escalation path from detection to board and regulatory notification.
- Materiality definition not documented; incident triage is ad hoc.
- Dual-regulated firms lack a coordination protocol between DFSA and FSRA or FCA obligations.

What good looks like

Defined escalation path	Hours-based internal escalation ladder from detection to SEO to regulatory notification, documented and tested.
Materiality definition	Written criteria for what constitutes a material incident, approved by compliance and risk.
Multi-regulator protocol	For cross-border firms: a documented coordination procedure for simultaneous notifications.

RISK: No documented internal procedure exists for 72-hour regulatory notification.

RISK: Compliance does not have DFSA ePortal access credentials pre-prepared for incident use.

RISK: Materiality thresholds not reviewed since the DFSA rules came into force in January 2024.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN: 72-hour notification | FSRA CRMF (Jan 2026): 24-hour notification | DORA (secondary lens for EU-nexus firms): 4-hour initial notification.	Missing or delayed regulatory notification triggers enforcement action independent of the incident itself. The process failure compounds the substantive failure.

PRACTICAL NEXT STEP
Verify that compliance holds active DFSA ePortal credentials. Confirm the internal escalation path is documented and that the materiality threshold is defined in writing. Test the notification procedure in the next CIRP exercise.

Q06 Are third-party and outsourced ICT risks actively governed, not just contractually managed?

Context

Third-party risk management consistently ranks as the most significant gap identified in DFSA thematic reviews, with implementation levels below 70% across the assessed population. The FSRA's 2026 CRMF introduces mandatory ICT service contract provisions. Both regulators distinguish between contractual coverage (necessary) and active governance (required). For wealth management firms, custody platforms, portfolio systems and cloud infrastructure typically represent the highest-concentration third-party exposures.

What breaks in practice

- Third-party risk is treated as a procurement and legal matter rather than an operational risk governance item.
- Vendor contracts contain security clauses but no ongoing monitoring, audit rights or performance metrics.
- Sub-contractor or fourth-party exposure is unknown; the vendor's own supply chain is unscrutinised.

What good looks like

Active register	Third-party ICT register maintained with criticality ratings, last review date and exit risk classification.
Contractual controls	ICT service contracts include: security standards, audit/inspection rights, incident notification obligations.
Ongoing monitoring	Critical vendors subject to periodic assurance, not solely at onboarding.

RISK: No third-party ICT risk register exists outside procurement records.

RISK: Key technology vendors have not been subject to assurance review in the past 24 months.

RISK: No contractual right to audit or inspect critical ICT providers.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA Thematic Review 2024: third-party risk as primary gap finding | FSRA CRMF: mandatory ICT contract provisions (Jan 2026) | DORA: ICT third-party risk chapter (secondary).	A supply-chain incident via an unmonitored vendor carries full regulatory exposure. The firm cannot demonstrate due diligence if controls were absent before the event.

PRACTICAL NEXT STEP
Request the current third-party ICT register. Identify the top five critical vendors by operational dependency. Confirm each has an active contract with audit rights and a documented last-review date. Escalate any gaps to the risk committee within 30 days.

Q07 Is the firm's cyber resilience testing programme proportionate and independently evidenced?

Context

The DFSA expects firms to maintain a comprehensive resilience testing programme for IT systems, including penetration testing, vulnerability assessments and testing of the incident response plan. For mid-sized regulated firms, the failure point is typically not absence of testing but lack of independence, insufficient scope (excluding cloud or third-party systems) or findings that are raised but not remediated within defined timeframes.

What breaks in practice

- Penetration testing conducted exclusively by internal IT staff with no independent external challenge.
- Testing scope excludes cloud-hosted systems or third-party platforms on grounds of vendor responsibility.

– Testing findings are tracked in IT but never reach the risk committee or board.

What good looks like

Independent testing	External penetration test conducted at least annually by a firm with appropriate credentials.
Full scope coverage	Testing scope covers internally hosted, cloud and critical third-party systems.
Findings governance	Testing findings classified by severity, remediation timelines set, and overdue items escalated to the risk committee.

RISK: Last external penetration test was more than 18 months ago.

RISK: Cloud infrastructure has never been included in the testing scope.

RISK: High-severity findings from the last test remain unresolved without documented risk acceptance.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA CRMF: comprehensive resilience testing programme | DFSA Business Plan 2023–24: regular testing including CIRP | UAE NCA: technical testing requirements.	Untested controls provide false assurance. A supervisory review that reveals testing gaps alongside a live vulnerability creates severe regulatory and reputational exposure.

PRACTICAL NEXT STEP
Request the most recent external penetration test report and remediation tracker. Confirm the testing scope included cloud and critical third-party systems. If high-severity open items exist, require a remediation timeline at the next risk committee.

Q08 Does the board receive meaningful, structured cyber risk reporting on a regular cadence?

Context

The DFSA's governance expectations require senior management at board and executive level to be continuously aware of cyber vulnerabilities, not briefed reactively. In practice, most board-level cyber reporting in mid-sized firms is either absent or consists of operational metrics that do not support governance decisions. The question is not whether boards receive reports; it is whether those reports enable them to exercise meaningful oversight.

What breaks in practice

- Cyber risk reporting is event-driven: the board only hears about cyber if something goes wrong.
- Reports are operationally dense: patch counts and ticket volumes, with no risk interpretation.
- No consistent reporting cadence; frequency varies by whoever prepares the briefing.

What good looks like

Regular cadence	Formal cyber risk update at every risk committee meeting, at minimum quarterly.
Board-level framing	Reports present risk posture, trend direction, open exceptions and regulatory compliance status, not operational metrics.
Escalation triggers	Reports include a clear escalation flag if any items have moved outside appetite.

RISK: The board has not received a structured cyber risk update in the past quarter.

RISK: The most recent cyber report was prepared by IT, not by risk or compliance, with no governance interpretation.

RISK: No standing agenda item for cyber risk at risk committee or board meetings.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN: senior management awareness obligation | DFSA Thematic Review 2024: governance dimension | G7 Element 2: governing authority access.	A board that cannot demonstrate awareness of cyber posture is exposed on both regulatory accountability and personal liability grounds under UAE governance rules.

PRACTICAL NEXT STEP
Review the last three risk committee packs. Confirm cyber risk appears as a standing item. If reporting is absent or purely operational, commission a one-page board-level cyber risk dashboard format for use from the next meeting cycle.

Q09 Is mandatory cyber awareness training completed annually by all staff, including the board?

Context

The DFSA requires annual mandatory cyber awareness training for all personnel. This includes non-technical staff and, critically, board members and senior executives. The failure mode in most firms is not absence of a training programme but selective coverage: front-office and IT complete training; board members, senior executives and new joiners fall outside the documented completion cycle. Regulators check records.

What breaks in practice

- Training completion is tracked for operational staff but not for board members or NEDs.
- Training content is generic, not contextualised to the firm's specific risk profile or the GCC threat landscape.
- Phishing simulation results are not fed into training calibration or risk committee reporting.

What good looks like

Universal coverage	100% completion tracked across all staff including board, NEDs and senior executives, with records retained.
Annual minimum	Completion cycle runs annually, with new-joiner training within 30 days of onboarding.
Contextualised content	Training reflects current threat intelligence relevant to GCC financial services firms.

RISK: Board member training completion rate is below 100% for the current cycle.

RISK: Training records cannot be produced for a specific individual on request.

RISK: Last training update predates the DFSA's January 2024 rule changes.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN: mandatory annual cyber awareness training | DFSA ePortal Cyber Thematic Review: training coverage assessed | UAE NCA: staff awareness requirements.	Selective training creates personal liability for individuals excluded and evidence of a cultural gap that regulators interpret as a systemic governance failure.

PRACTICAL NEXT STEP

Request the training completion register for the current cycle, filtered to show board members and NEDs specifically. If any are incomplete, close the gap before the next supervisory contact or audit cycle. Retain the evidence.

Q10 Has the firm assessed its cyber obligations across all applicable regulatory jurisdictions?

Context

Many GCC-based financial services firms operate under multiple regulatory frameworks simultaneously: DFSA (DIFC), FSRA (ADGM), CBUAE, UAE NCA and, for firms with cross-border activities, FCA SYSC or DORA obligations. These regimes are not interchangeable. The DFSA is principles-based with prescriptive incident notification rules. DORA is highly prescriptive across all dimensions. The FSRA's January 2026 CRMF introduces requirements that go further than the DFSA in several areas, including contract provisions and 24-hour notification. Compliance with one does not guarantee compliance with another.

What breaks in practice

- The firm treats DFSA compliance as satisfying all regulatory cyber obligations.
- No regulatory mapping exercise has been conducted to identify material differences between applicable regimes.
- Cross-border notification obligations are not coordinated, creating timing conflicts under pressure.

What good looks like

Regulatory matrix	A documented mapping of applicable cyber obligations across each relevant regime, reviewed annually.
Gap identification	Material differences between regimes (e.g. DFSA 72-hour vs FSRA 24-hour notification) explicitly identified and controlled.
Compliance monitoring	Changes to any applicable regime are tracked and the matrix updated within a defined review cycle.

RISK: No cross-jurisdictional regulatory mapping exists.

RISK: The firm is unaware that the FSRA's CRMF (effective January 2026) introduced requirements materially different from the DFSA.

RISK: DORA obligations for EU-nexus activities have not been assessed.

REGULATORY REFERENCE	BOARD ACCOUNTABILITY RISK
DFSA GEN (DIFC) | FSRA CRMF effective Jan 2026 (ADGM) | CBUAE Operational Risk | UAE NCA Cybersecurity Framework | FCA SYSC / DORA (secondary where applicable).	Operating under the assumption that one regulatory compliance position covers all applicable jurisdictions creates material blind spots and unquantified enforcement risk.

PRACTICAL NEXT STEP
Ask compliance to produce a one-page regulatory mapping table showing: applicable regimes, key cyber obligations per regime, material differences and current compliance status. If no such document exists, commission it as a priority action.

Cross-Cutting Themes

Across the ten questions, four systemic patterns consistently differentiate firms with defensible cyber governance from those with structural exposure:

Governance is the control	The majority of DFSA thematic review findings relate to governance failures, not technical gaps. Boards that treat cyber as a technology function rather than a risk governance matter are consistently more exposed. The framework, the risk appetite, the incident response plan and the reporting structure must all carry board-level ownership.
Documentation without evidence is not compliance	Written policies and frameworks are necessary but insufficient. Regulators assess whether controls work: they look for tested procedures, completion records, board minutes, exercised response plans and remediated findings. The absence of evidence is treated as the absence of control.
Third-party risk remains the most persistent gap	Both the DFSA and FSRA have identified third-party ICT risk as the most widespread governance gap across the regulated population. Contractual coverage is not the same as active governance. Firms must demonstrate ongoing monitoring of critical vendors, not solely due diligence at onboarding.
Regulatory obligations are multiplying, not converging	The January 2026 FSRA CRMF, DORA's reach into GCC-based firms with EU-entity connections, and the DFSA's active thematic review programme mean that the compliance floor is rising. Firms that map their obligations once and do not revisit them are accumulating unquantified risk silently.

About Daniel Young Advisory

Daniel Young Advisory is the practice of Daniel Young, a Strategic IT Director and CIO based in Dubai, specialising in technology risk, resilience and regulatory compliance for regulated firms operating under the DFSA and FCA.

If this checklist has identified gaps in your firm's cyber governance position, the following engagement models are directly relevant:

Risk & Resilience Review - An independent executive-level assessment of your technology risk posture, covering governance maturity, incident readiness and regulatory alignment. Delivers a board-ready remediation roadmap with defined risk trade-offs. Directly addresses gaps identified in Questions 1, 2, 4, 5, 7 and 8.

Vendor Strategy - Executive oversight of your ICT third-party landscape, covering contract governance, audit rights and ongoing monitoring. Directly addresses gaps identified in Question 6.

CIO Leadership - Interim IT Director or CIO mandate for firms requiring executive-level technology leadership through a period of regulatory change or operational scaling.

Initial conversations are without obligation. Contact via danielpyoung.com or linkedin.com/in/daniel-p-young.

Website	danielpyoung.com
LinkedIn	linkedin.com/in/daniel-p-young
Enquiries	Via the website contact form

Disclaimer

FREELY AVAILABLE RESOURCE This document is published by Daniel Young Advisory as a free resource. It may be shared, forwarded, or reproduced in full provided it is attributed to Daniel Young Advisory and not altered. Commercial resale or rebranding without prior written consent is prohibited.

DISCLAIMER & LIMITATION OF LIABILITY This document is provided for informational purposes only. It does not constitute legal, regulatory, financial or technical advice. Regulatory requirements change; readers should verify current obligations with qualified legal and compliance advisers. While every effort has been made to ensure accuracy as at March 2026, Daniel Young Advisory makes no warranties regarding completeness or continuing accuracy, and accepts no liability for any loss or damage arising from reliance on this document.

GOVERNING LAW This document shall be governed by and construed in accordance with the Federal Laws of the United Arab Emirates as applicable in the Emirate of Dubai.