May 20th 2026

SUBMITTED VIA SURVEY

To whom it may concern,

**Re: DFSA Consultation Paper No. 170 on Operational Resilience**

## About Global Digital Finance (GDF)

GDF is the leading global members association advocating and accelerating the adoption of best practices for crypto and digital assets. GDF's mission is to promote and facilitate greater adoption of market standards for digital assets through the development of best practices and governance standards by convening industry, policymakers, and regulators.

The input to this response has been curated through a series of member discussions, industry engagement, and previous engagement with the UK public sector over the years and GDF is grateful to its members who have taken part.

As always, GDF remains at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail with our members.

Yours faithfully,
Elise Soucie Watts – Executive Director – GDF

## Response to the Public Consultations: Executive Summary

Global Digital Finance welcomes the DFSA's proposed operational resilience framework and supports the requirement for Authorised Persons to regularly identify critical business services as part of a proportionate, risk-based approach aligned with international standards. We agree that governing bodies should oversee and approve both the identification of critical business services and the setting of impact tolerances, ensuring operational resilience is embedded at a strategic level.

We support the DFSA's principles-based and flexible framework, particularly regarding impact tolerances, mapping of critical resources, and scenario testing. At the same time, we encourage additional clarity in the Supervisory Guidelines to ensure proportionality for smaller firms, recognition of group-level governance structures, and practical guidance on near-miss reporting thresholds and reassessment triggers.

From the perspective of digital asset firms, we recommend that the framework explicitly recognise the unique operational dependencies associated with blockchain infrastructure, smart contracts, and custody arrangements. We also encourage the DFSA to maintain a technology-neutral approach, allow reliance on recognised third-party testing, and support collaborative resilience testing where services depend on shared infrastructure.

Overall, we believe the proposed 24-month implementation period is broadly appropriate, provided supervisory expectations remain proportionate and firms are given sufficient time and clarity to implement the framework effectively.

**Response to the Consultation Paper Questions**

**Question 1: Do you agree that an Authorised Person should perform a regular exercise to identify its critical business services?**

Overall, GDF welcomes the DFSA's proposal to introduce an operational resilience framework for the DIFC and supports the requirement for Authorised Persons to carry out a regular exercise to identify their critical business services. The approach is consistent with international standards, in particular Basel Core Principle 25 and the Basel Principles for Operational Resilience, and reflects the model adopted across leading regulatory jurisdictions including the UK, Singapore and Hong Kong.

GDF particularly welcomes the two-tier structure, where the obligation to conduct the identification exercise applies universally, but the full suite of resilience requirements applies only to those Authorised Persons that identify a critical business service. This is a proportionate and risk-based approach that appropriately reflects the diversity of firms regulated by the DFSA, and GDF encourages the DFSA to maintain this structure in the final rules.

We note, however, that paragraph 23 of the Consultation Paper introduces a supporting classification framework ("Likely", "May", "Unlikely") to assist firms in determining whether they have critical business services. While this is intended to reduce the risk of over-identification, it may in practice result in firms within the "May" category undertaking a more detailed assessment in order to determine whether any critical business service is present.

In such cases, firms may conclude, following assessment, that no critical business service has been identified, but would nevertheless be expected to document their reasoning, obtain appropriate Governing Body oversight, and repeat the exercise at appropriate intervals. While GDF recognises that a documented and appropriately governed conclusion is important from both a governance and legal perspective, we consider that this may give rise to a disproportionate administrative burden for smaller or less complex firms, depending on how the expectation is applied in practice.

We therefore encourage the DFSA to consider whether the finalised Supervisory Guidelines could provide additional clarity on the level of assessment expected in such cases, including whether a more proportionate and streamlined approach may be appropriate for firms in the "May" and "Unlikely" categories. This could support a defensible and appropriately governed outcome without requiring firms to replicate, in full, the more detailed processes that may be appropriate for firms that are more likely to identify critical business services.

Finally, we recommend that the finalised Supervisory Guidelines confirm that the assessment should be anchored in harm and systemic impact as the primary criteria, rather than the scale or complexity of a firm's operations in isolation. A smaller firm providing a custody or payment service for which there is limited substitutability in the DIFC market may carry a higher criticality profile than a larger, more diversified firm whose services are readily available from other providers. GDF also recommends that the Supervisory Guidelines include one or two illustrative examples drawn from digital asset activities within

Annex B, alongside the existing examples, to support consistent application of the framework across the full population of Authorised Persons. For instance, crypto token custody and digital asset settlement services are activities already captured within the Table 1 categories of Providing Custody and Operating an Exchange, and a brief acknowledgement of this in the Guidelines would be beneficial to reduce unintended interpretive uncertainty for firms in that sector without requiring any departure from the existing analytical framework.

We also note that the Consultation Paper leaves the frequency and triggers for reassessment to be further specified in the Supervisory Guidelines. In this regard, we encourage the DFSA to provide additional clarity that reassessment should be undertaken not only on a periodic basis, but also in response to material changes in a firm's business model or operating environment. This could include, for example, the introduction of new products or services, material outsourcing or third-party arrangements, or significant corporate restructuring.

Providing clarity on such event-driven triggers would support firms in maintaining an accurate and up-to-date assessment of their critical business services over time, and would be consistent with approaches adopted in other jurisdictions, including the UK framework under SYSC 15A.2.2.

**Question 2: Do you agree that the Governing Body should be responsible for approving the outcome of the critical business services identification exercise?**

We agree that the Governing Body should be responsible for approving the outcome of the critical business services identification exercise. Placing this responsibility at board level is consistent with the governance expectations of international standards and ensures that operational resilience is treated as a strategic matter rather than a purely operational one. GDF supports this approach.

Further to this, we recommend that the Supervisory Guidelines provide clarity on how this expectation applies to Authorised Persons that operate as part of a larger group, where governance responsibilities may be shared between the DIFC entity and a parent or group board. In such cases, GDF considers that the DFSA should recognise group-level board approval as satisfying this requirement, provided that the DIFC entity's Governing Body has had meaningful input into the assessment and retains clear accountability for the outcome as it relates to the firm's DIFC-regulated activities. A rigid requirement for a standalone DIFC board approval process, irrespective of group governance arrangements, could create unintended duplication and is not likely to materially improve supervisory outcomes.

**Question 3: Do you agree that an Authorised Person should set an impact tolerance for each critical business service identified?**

Yes, we agree that an Authorised Person should set an impact tolerance for each critical business service identified. The requirement to define in advance the maximum level of disruption that is tolerable is a core element of effective operational resilience frameworks and is consistent with the approach taken by

the PRA, FCA, MAS and other leading regulators. It also ensures that impact tolerances are embedded in governance and operational planning, rather than assessed retrospectively following a disruption.

We welcome the flexibility in Annex C of the Supervisory Guidelines, which allows firms to select from a range of metrics including downtime, number of transactions affected, number of users affected, and financial or data losses. This reflects the reality that different business services will have materially different risk profiles, and that a single mandatory metric would not be appropriate across the diverse population of Authorised Persons in the DIFC.

On this point, we would encourage the DFSA to confirm in the finalised Supervisory Guidelines that firms may give primacy to transaction-value or transaction-volume metrics where these are more meaningful than time-based metrics for the business service in question. For certain digital asset services, including settlement and custody, the value of assets at risk during a disruption may be a more relevant indicator of harm than the duration of an outage. The current footnote 2 to Annex C, which states that the time-based metric should be part of any multi-metric selection where relevant, is helpful, but we would also recommend that the Guidelines make equally clear that time-based metrics need not be the primary measure where another metric better captures the materiality of the risk.

**Question 4: Do you agree that the Governing Body should be responsible for approving the impact tolerances?**

We agree that the Governing Body should be responsible for approving the impact tolerances. As with the identification exercise, board-level approval ensures that tolerance thresholds are set with appropriate seniority and that senior leadership takes accountability for the level of disruption the firm is prepared to accept in respect of each critical business service. This is consistent with international best practice and with the governance expectations that apply in comparable frameworks.

We also welcome the expectation in paragraph 12 of the Supervisory Guidelines that, once approved, impact tolerances are cascaded to senior management and the people involved in the delivery of the relevant critical business service. This is an important practical step that helps ensure tolerances are operationally meaningful rather than remaining purely as board-level documentation.

We would also respectfully note the same consideration raised in our response to Question 2 here. Where an Authorised Person operates as part of a larger group, we encourage the DFSA to also recognise group-level board approval as satisfying this requirement, provided that the DIFC entity's Governing Body has had meaningful input and retains clear accountability for the tolerances as they relate to the firm's DIFC-regulated activities.

**Question 5: Do you agree that an Authorised Person should map out and document the minimum set of resources required to deliver critical business services within impact tolerances?**

GDF agrees that an Authorised Person should map out and document the minimum set of resources required to deliver critical business services within impact tolerances. Mapping is an essential component of any operational resilience framework, as it enables firms to identify vulnerabilities, single points of failure, and concentration risks before a disruption occurs rather than in response to one. The requirement is consistent with international standards and with the approach taken by comparable regulators.

We also welcome the principles-based approach adopted in paragraph 13 of the Supervisory Guidelines, which focuses on the end-to-end delivery of a critical business service and identifies people, processes and technology as the core resource categories. We encourage the DFSA to maintain this technology-neutral framing in the finalised Guidelines and to resist prescribing specific technical configurations or architectural requirements, as the appropriate approach will vary significantly across firm types, business models and the technologies they rely upon. This includes confirming that a process-level mapping approach satisfies the requirement, without mandating exhaustive system-by-system architectural documentation.

On third-party dependencies, we note that paragraph 13 of the Supervisory Guidelines identifies intra-group and external third-party arrangements as typically requiring particular attention in the mapping exercise. We support this but recommend that the Guidelines provide further clarity on how firms should approach dependencies on infrastructure that operates outside of any contractual relationship with the firm. For digital asset firms in particular, critical business services may depend in part on blockchain network infrastructure, validator sets, or smart contract logic that is not provided by a contractually bound third party and cannot be directed or substituted by the firm in the way that a traditional outsourcing arrangement can. We consider that accountability for mapping should attach to matters within the firm's control, and that the Guidelines should confirm that firms are not expected to document or remediate dependencies on decentralised infrastructure where those dependencies cannot be influenced through governance or contractual arrangements. Where such dependencies exist, firms should instead be expected to assess and document the associated risks and to reflect them in their scenario testing.

We also recommend that the Guidelines clarify that the mapping exercise should be proportionate to the firm's size, complexity and risk profile. The depth and granularity of documentation that is appropriate for a systemically significant exchange will differ considerably from that appropriate for a smaller custody or payment firm, and the Guidelines should make clear that a proportionate methodology, developed by the firm to reflect its own business, will satisfy the requirement.

**Question 6: Do you agree that an Authorised Person should test its ability to remain within impact tolerances under severe but plausible scenarios?**

Yes, overall, we agree that an Authorised Person should test its ability to remain within impact tolerances under severe but plausible scenarios. Scenario testing is the mechanism through which the mapping exercise is validated in practice, and it is only through testing that firms can identify whether their

planned response to a disruption would actually enable continued delivery of a critical business service within the set tolerance. We support the requirement and welcome its inclusion as a core element of the framework.

We welcome the flexibility in paragraph 15 of the Supervisory Guidelines, which expects firms to consider an appropriate range of adverse circumstances of varying nature, severity and duration, relevant to their business profile. This outcomes-based approach is appropriate, and we encourage the DFSA to maintain it in the finalised Guidelines. Prescribing a fixed set of mandatory scenarios would risk firms treating the exercise as a compliance exercise rather than a genuine test of their resilience and would not reflect the materially different risk profiles across the DIFC's diverse population of Authorised Persons.

On scenario design, we recommend that the finalised Guidelines acknowledge that firms operating digital asset services may face an operational risk profile that differs in certain respects from traditional financial services firms, and that scenario selection should reflect the specific characteristics of the business model in question. For digital asset firms, relevant scenarios may include disruptions to custody infrastructure or key management systems, failures in smart contract logic, or simultaneous disruption across interconnected services of the kind identified in paragraph 16 of the Supervisory Guidelines. The principles-based approach in paragraph 15 is well suited to capturing this diversity, and we encourage the DFSA to confirm in the finalised Guidelines that firms are expected to select scenarios that genuinely reflect their own risk profile rather than defaulting to scenarios designed primarily with traditional financial services in mind

Finally, GDF would also recommend that the Guidelines confirm that collaborative testing approaches are permissible where a firm's critical business service depends on shared infrastructure or on services provided by other regulated entities. Requiring firms to test entirely in isolation would not reflect operational reality and could produce misleading results where the resilience of a service depends in part on the response of a third party or counterparty. Where collaborative testing is carried out, firms should remain responsible for documenting their own findings and conclusions.

In addition, GDF recommends that the Guidelines confirm that a firm may place reasonable reliance on testing carried out by a third-party provider, where that testing has been conducted in accordance with recognised industry standards. This would be consistent with approaches adopted in other jurisdictions and reflects the practical reality that, for certain critical dependencies, a firm may not be in a position to conduct independent testing of third-party infrastructure.

Where a firm relies on third-party testing in this way, it should satisfy itself that the scope and methodology of that testing are relevant to its own critical business services, retain appropriate documentation of the results, and take into account any identified gaps or residual risks in its own resilience planning. Reliance on such testing should not remove the firm’s responsibility for assessing its operational resilience or for taking appropriate remedial action where vulnerabilities are identified.

**Question 7: Do you agree that an Authorised Person should notify the DFSA of disruptions to critical business services when it has breached or has come close to breaching its impact tolerance?**

We agree that an Authorised Person should notify the DFSA of disruptions to critical business services where it has breached its impact tolerance. Timely notification enables the DFSA to assess whether coordinated action or market communication is necessary and supports the regulator's ability to monitor systemic risk across the DIFC financial services industry. We support the requirement and its inclusion in the framework.

We recommend that the DFSA provide further guidance on what constitutes having come "reasonably close" to breaching an impact tolerance, or alternatively remove the wording completely as it would be difficult to provide any guidance on the such. This threshold will determine the practical scope of the notification obligation for most firms in most disruption scenarios. The concept of a near-miss notification is well established in comparable frameworks, but the calibration of the threshold matters considerably. Too low a threshold risks generating a high volume of notifications of limited supervisory value, while too high a threshold risks material disruptions going unreported until after the tolerance has been breached. We recommend that the finalised Supervisory Guidelines set out indicative parameters for what the DFSA would consider to constitute proximity to a breach, with reference to the metrics and tolerances set by the firm, to give Authorised Persons a workable basis for making this assessment in practice.

We also recommend that the finalised Supervisory Guidelines provide further clarity on the practical application of the immediate notification requirement, including what would constitute timely notification in the context of a fast-moving disruption. In particular, indicative timeframes or benchmarks could be helpful in supporting a consistent interpretation of supervisory expectations across firms.

We also encourage the DFSA to clarify that the notification obligation is triggered from the point at which a firm has determined, on a reasonable basis, that a disruption has breached or is approaching its defined impact tolerance. This would provide firms with a clearer and more operationally workable basis for meeting the expectation to notify as soon as reasonably practicable, while maintaining appropriate flexibility to reflect the circumstances of the disruption.

Finally, we also encourage the DFSA to consider how the notification framework can support broader information sharing across the DIFC financial services community following a material disruption, particularly where a disruption may affect multiple firms simultaneously or in rapid succession. Public-private coordination mechanisms of this kind would complement the bilateral notification requirement and would strengthen the collective resilience of the DIFC ecosystem, consistent with the DFSA's objectives of maintaining stability and confidence in the financial services industry.

**Question 8: Do you agree with the proposed implementation period?**

We consider the proposed 24-month implementation period to be broadly reasonable and welcome the DFSA's recognition that Authorised Persons will require adequate time to make the necessary

arrangements to comply with the new requirements. The phased approach, with substantive progress on identification, impact tolerance setting, mapping and initial scenario testing expected within the first 12 months, provides a sensible structure for implementation.

In addition to this GDF recommends that the DFSA confirm that the implementation timeline will be applied proportionately, with supervisory expectations during the implementation period calibrated to the size, complexity and resources of the firm. We would recommend that for smaller firms, and firms for whom this framework represents a more significant operational change, that the DFSA exercise flexibility in supervisory expectations so that firms can sequence their implementation in a way that reflects their individual circumstances, provided they are making demonstrable and documented progress toward full compliance.

We also note that the 24-month period runs from the date the rules are enacted rather than from the close of the consultation period. Given that the consultation closes on 26 May 2026, and that the process of finalising the rules and publishing the final Supervisory Guidelines will take additional time, the effective implementation window available to firms may be shorter in practice than the headline figure suggests. We encourage the DFSA to be mindful of this when setting the enactment date, and to ensure that firms have sight of the final rules and Guidelines with sufficient lead time to begin their implementation planning in earnest.

We also note that the Consultation Paper provides limited detail on how the DFSA intends to use the information generated through the framework in practice, including the outcomes of identification exercises, mapping documentation, and disruption notifications. Greater clarity in this area would assist firms in understanding how supervisory expectations are likely to be applied in practice, which is an important consideration when making investment decisions in resilience capabilities across people, systems, and third-party arrangements.

In this context, we encourage the DFSA to consider whether it may be appropriate to share aggregated or anonymised thematic insights during and following the implementation period. This could provide firms with a useful reference point for benchmarking and continuous improvement, support more consistent implementation across the DIFC, and reinforce the collaborative objective of strengthening operational resilience at a market-wide level.