20 March 2026

SUBMITTED VIA EMAIL: ra.consultation@adgm.com

To whom it may concern,

Re: ADGM FSRA Discussion Paper No. 1 of 2026: Proposed Guidance on Crypto Mining Activities

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 MEA 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 Discussion Paper: Executive Summary

GDF welcomes the Abu Dhabi Global Market (ADGM) Financial Services Regulatory Authority's Discussion Paper on Proposed Guidance on Crypto Mining Activities and the opportunity to contribute to this consultation. We are broadly supportive of the objectives the Guidance seeks to advance, including establishing risk-based, proportionate and transparent supervisory expectations for commercial crypto mining activities conducted within or from ADGM. The emphasis on governance, operational integrity and corporate transparency is consistent with international best practice, and the registration-based approach is a measured and appropriate supervisory model for this sector.

Our response identifies a number of areas where targeted clarification or refinement would materially strengthen the Guidance. The most important concerns the definition of the regulatory perimeter. As currently drafted, the Guidance does not clearly distinguish between Proof-of-Work mining, enterprise Proof-of-Stake validator operations, incidental node operations, and supporting infrastructure services that do not directly generate block rewards. These activities present materially different risk profiles, and an explicit perimeter description, accompanied by a non-exhaustive out-of-scope list, would significantly reduce regulatory uncertainty and the risk of unintended perimeter capture for firms engaged in multi-functional digital asset activities.

Across the substantive provisions, we support the principles-based approach adopted for security controls, pre-licensing assessment, general licence conditions and supervisory oversight. We recommend against prescriptive technical baselines in favour of standards-aligned frameworks, and we encourage proportionality by scale throughout. We raise specific concerns around: the granularity and security sensitivity of on-chain address disclosure, and the importance of confidentiality safeguards; the need for materiality thresholds governing outsourcing, overseas footprint and energy arrangement notifications, rather than broad prior-approval triggers; and the importance of grounding consolidated overseas disclosure obligations in governance nexus and materiality, rather than allowing them to evolve into expectations that extend beyond ADGM’s supervisory nexus. On each of these points, our recommendations are designed to preserve supervisory effectiveness while supporting the operational agility and commercial confidence that will sustain ADGM's position as a leading jurisdiction for responsible digital asset activity.

GDF and its members remain available to discuss any aspect of this response and would welcome further engagement with the FSRA as the Guidance is finalised.

Responses to Discussion Paper Questions:

Section 1

Q1: Are the objectives and scope of this Guidance clear and sufficient? Which areas, if any, require further clarification?

GDF considers the overall objectives of the Guidance to be clear and well-articulated. The document appropriately seeks to establish baseline governance, transparency and supervisory expectations for commercial crypto mining activities conducted within or from ADGM, while recognising the operational and technical characteristics of this sector. The emphasis on risk-based supervision, operational integrity and corporate transparency is consistent with international best practice.

However, we believe additional clarification around scope would materially strengthen the Guidance and reduce the risk of unintended perimeter capture.

Clarifying the Intended Activity Perimeter

As currently drafted, the Guidance appears primarily oriented toward Proof-of-Work (PoW) mining operations involving physical infrastructure, ASIC procurement, energy management and hash rate generation associated with block production and reward generation. If this is the intended regulatory focus, we would recommend that this be stated expressly.

In particular, clarification would be helpful in distinguishing between:

- Proof-of-Work mining (the main intended perimeter).
- Pure Proof-of-Stake (PoS) validator operations, particularly enterprise validator clusters where the core risks relate primarily to validator key management and signing security, slashing governance, validator uptime and protocol participation, rather than physical plant, energy consumption or hardware supply chains.
- Incidental node or validator operations conducted as part of another regulated or commercial activity (e.g. exchanges, custodians, developers or research teams operating nodes for resiliency, monitoring, governance participation, network connectivity or testing).
- Infrastructure services that support network participation but do not directly generate block rewards (for example monitoring nodes, relay infrastructure, or network-health analytics).

These activities present materially different operational and risk characteristics and may warrant distinct regulatory treatment.

Out-of-Scope Clarification

Additionally, we would also welcome the inclusion of a clear, non-exhaustive "out of scope" list to provide legal certainty. This could include, for example:

- Non-reward full nodes.
- Testnet, research or security monitoring nodes.
- Incidental validators not offered as a third-party commercial service.
- Open-source protocol development activities.

Providing such clarity would reduce the risk of capturing low-risk technical infrastructure activity that does not constitute commercial mining in any meaningful sense.

Importance of Perimeter Certainty

A well-defined scope is particularly important in a rapidly evolving ecosystem where mining, validation and node operations can overlap. Clear perimeter boundaries will:

- Avoid regulatory uncertainty for firms engaged in multi-functional digital asset activities.
- Prevent disproportionate licensing requirements for low-risk or incidental operations.
- Ensure supervisory resources remain focused on activities that present material operational, governance or integrity risks.

Overall, while the objectives of the Guidance are clear and appropriate, and we are supportive of their intent, we recommend that the RA provide additional clarity around the intended activity perimeter and explicitly identify categories of activity that fall outside scope. This would enhance certainty, proportionality and effective implementation.

Q2: Is the treatment of small-scale, non-commercial mining as generally out of scope appropriate and proportionate?

Yes, GDF supports the proposed treatment of small-scale, non-commercial mining activities as generally out of scope of the regulatory perimeter. We consider this approach to be both proportionate and appropriate.

Drawing a clear distinction between commercial mining operations conducted as a business and small-scale, hobbyist or incidental activity reflects a risk-based supervisory philosophy. Non-commercial mining conducted at a de minimis scale does not typically present the governance, consumer protection, financial crime, or market integrity risks that justify regulatory oversight at

an institutional level, particularly where activities involve self-operated hardware and do not involve third-party service provision or custody of client assets. Bringing such activity within scope could create unnecessary compliance burdens without delivering commensurate regulatory benefit.

We also consider that this approach aligns with international practice, where regulatory frameworks for digital asset activities increasingly focus on organised, profit-seeking enterprises rather than individual or experimental activity. Maintaining this distinction helps avoid regulatory overreach and supports innovation and technological literacy at the individual level, while preserving the Registration Authority's ability to supervise entities whose scale, structure or commercial orientation may create broader risks.

That said, clarity around the thresholds and indicators distinguishing non-commercial from commercial activity will be important. Such indicators could include factors such as scale of hash power or validator capacity deployed, whether services are offered to third parties, whether dedicated commercial infrastructure is used, or whether the activity generates material and recurring revenue. Transparent criteria will support consistent application and reduce uncertainty for participants assessing whether licensing requirements apply.

Overall, we agree that excluding small-scale, non-commercial mining from the regulatory perimeter represents a measured and proportionate policy choice consistent with ADGM's principles-based and risk-sensitive regulatory approach.

Section 2

Q3: Do you agree with the baseline policy principles for responsible mining operations, including governance, compliance, and operating strictly within licence boundaries?

GDF supports the baseline policy principles set out in the Discussion Paper and the accompanying proposed guidance. We consider these principles to be proportionate, well-calibrated and aligned with international best practice in relation to governance, transparency and supervisory oversight of digital asset market participants.

We also agree with the emphasis placed on full compliance with ADGM legislation, including timely filings, disclosures and ongoing reporting obligations. Consistent and transparent supervisory engagement supports confidence in the regulatory framework and the credibility of the broader digital asset ecosystem within the jurisdiction.

The proposed expectations relating to corporate governance and record-keeping are similarly appropriate. Mining operations, particularly at scale, can involve complex ownership structures, cross-border equipment procurement, power supply arrangements, hosting agreements and infrastructure management across multiple jurisdictions. Requiring accurate and comprehensive business records, alongside governance frameworks that enable firms to demonstrate ongoing compliance at any time, reflects sound supervisory practice and mirrors expectations applied across other regulated financial and commercial activities within ADGM.

In applying these baseline principles, we would encourage calibration by reference to consensus mechanism and operational model. Proof-of-Work (PoW) mining is primarily characterised by industrial-scale infrastructure, physical security, energy procurement, hardware supply chain management and facility resilience. By contrast, Proof-of-Stake (PoS) validator operations are principally exposed to cryptographic key management risk, validator uptime and slashing governance, client software integrity and protocol participation dynamics. While the overarching governance and compliance expectations should apply consistently, the specific control environment and supervisory emphasis should reflect these materially different risk drivers. This approach would ensure that supervisory expectations remain proportionate while recognising the differing operational characteristics of infrastructure-based mining and validator participation. Such calibration would enhance proportionality and ensure that the Guidance remains technology-neutral while responsive to operational realities.

Importantly, these principles do not appear to impose undue operational burdens. Rather, they articulate baseline standards that responsible operators should already meet as part of good corporate hygiene and risk management. By setting clear supervisory expectations from the outset, ADGM provides regulatory certainty while reinforcing its position as a jurisdiction committed to high standards, transparency and sustainable growth in digital asset activities.

We therefore support the baseline policy principles as drafted and consider them an appropriate foundation for the RA's supervisory approach to crypto mining activities.

Q4: Should minimum security control baselines be specified, for example access control, key management for reward addresses, network segmentation, logging, and incident response?

GDF does not consider it necessary at this stage to prescribe detailed minimum security control baselines in the form of mandated technical requirements (e.g., specific access control configurations, key management architectures, network segmentation models, logging standards or incident response procedures).

We consider that the approach set out in the proposed Guidance under Section 2.1, requiring robust cybersecurity and operational controls, adherence to recognised international cybersecurity frameworks, and implementation of best practices for physical and operational security, is proportionate and appropriate.

Mining operations vary significantly in scale, infrastructure model, geographic footprint, hosting arrangements, custody design for reward addresses, and degree of vertical integration. A highly prescriptive, rule-based baseline could risk being either under-inclusive (quickly outdated or technically insufficient) or over-inclusive (imposing rigid controls that are disproportionate for certain operating models). Given the pace of technological development in hardware security, firmware design, network architecture and key management tooling, overly detailed regulatory specifications may rapidly become obsolete.

A principles-based framework is likely to be more effective and future-proof if it:

- Requires firms to adopt recognised international cybersecurity frameworks or standards;
- Expects demonstrable risk assessment and mitigation processes; and
- Empowers the Registration Authority to assess the adequacy of controls on a case-by-case basis.

If the RA considers it helpful to provide further clarity, we would suggest that this takes the form of non-binding guidance or illustrative best practice examples rather than mandatory technical baselines.

In that context, there are certain control areas that consistently arise in mining and validator-related incidents and could be referenced as good-practice themes within guidance (without becoming rigid requirements). These include:

- *Firmware and supply-chain integrity controls*, including verification of hardware provenance, firmware authenticity and secure update processes.
- *Segregation of operational environments*, particularly separation between mining/validator infrastructure, administrative systems and treasury or wallet environments.
- *Key management controls mapped to the underlying consensus mechanism*, recognising that Proof-of-Work operations primarily face infrastructure and facility security risks, whereas Proof-of-Stake validators face heightened exposure to private key compromise, slashing conditions, uptime governance and client software vulnerabilities.

These themes reflect the types of control failures that have historically contributed to mining and validator infrastructure incidents. Referencing such themes at a high level would signal supervisory priorities while preserving technological neutrality and flexibility.

Furthermore, as noted under the pre-licensing requirements, the RA may request a Detailed Operational Plan containing further information on the firm's technical architecture and operational arrangements necessary to assess the application.

Overall, in our view the proposed principles-based approach, coupled with appropriate pre-licensing review where necessary, appropriately balances security, flexibility and innovation, and we therefore do not consider additional prescriptive minimum baselines to be necessary at this time.

Section 3

Q5: Are the proposed pre-licensing information and assessment areas set out under section 3 appropriate and sufficient? Which elements require more detail or clearer evidence expectations?

GDF considers the proposed pre-licensing information and assessment areas under Section 3 to be broadly appropriate, proportionate and aligned with the Registration Authority's (RA) objective of ensuring responsible and transparent mining operations within ADGM.

The requirement to obtain a Commercial Licence specifying "Crypto Mining" (or an equivalent activity code) provides helpful perimeter clarity. This reduces ambiguity around the nature of the authorised activity and supports effective supervision.

We are generally supportive of the three core assessment areas identified:

1. **Detailed Operational Plan**: Requiring applicants, particularly larger-scale operators, to provide technical specifications, projected scale, operational workflows and a risk management framework is appropriate as noted above under the previous questions. Mining operations can involve significant infrastructure investment, energy usage, cross-border supply chains, hosting arrangements and specialised hardware deployment. Ensuring that firms demonstrate operational preparedness and risk awareness at the outset supports both supervisory confidence and long-term operational resilience.

2. **Infrastructure, Security & Resilience Plan:** The expectation that applicants articulate physical security measures, cybersecurity controls aligned with recognised international standards (e.g. ISO 27001, NIST), and business continuity/disaster recovery arrangements is consistent with global best practice. Given the operational concentration

risk that may arise in large-scale facilities, upfront resilience planning is prudent.

3. **Disclosure of On-Chain Assets:** Requiring disclosure of blockchain wallets or smart contract addresses owned or controlled by the entity is proportionate from a transparency and supervisory monitoring perspective.

Areas Where Further Clarity May Be Helpful

While we do not see fundamental concerns with the structure of the proposed requirements, we suggest the following refinements to enhance proportionality and legal certainty:

- **Proportionality by Scale:** It would be helpful to clarify that the depth and granularity of information required will be calibrated according to the scale, operational complexity and potential systemic footprint of the proposed operation. Smaller commercial operators should not be subject to the same level of documentary burden as industrial-scale facilities unless justified by risk.
- **Precision of Technical Disclosures:** Certain detailed disclosures, such as exact facility specifications, hardware configurations or efficiency metrics, may create both physical security risks (e.g., facility targeting) and commercial sensitivity. Additionally, mining operations frequently reconfigure hardware fleets, firmware versions, hosting arrangements, mining pools and energy optimisation strategies. Requiring highly granular, static technical inputs at licensing stage may inadvertently create repeated resubmission cycles as configurations evolve.

  A practical solution would be to permit disclosure of ranges, architectural descriptions or high-level design summaries at the licensing stage, with more detailed technical information available to the RA upon request where specific risk indicators justify deeper supervisory review.

- **Clear Evidence Expectations:** Further guidance on what constitutes sufficient evidence, for example, whether draft policies or implementation roadmaps are acceptable at application stage, or whether fully implemented frameworks must already be in place, would assist applicants in preparing submissions efficiently and avoid iterative information requests.
- **Confidentiality Safeguards (On-Chain Disclosure):** With respect to disclosure of wallet addresses and smart contracts, clarity around how such information will be safeguarded and used by the RA would be welcome. While transparency to the regulator is appropriate, wallet address disclosure can reveal commercially sensitive operational information, including revenue flows, counterparties, and treasury management practices.

Explicit confirmation of confidentiality protections and secure handling procedures would strengthen confidence in this requirement.

- **Ongoing vs. Point-in-Time Disclosure:** It may also be helpful to clarify whether wallet disclosures are expected solely at the point of application, or on an ongoing basis as new addresses are generated. Mining operations may rotate or segregate addresses for operational security and treasury management reasons.

Overall, we consider the proposed assessment areas to be appropriate and sufficiently comprehensive to enable effective supervisory review. With minor clarification around proportionality, evidentiary expectations and confidentiality protections, the framework would provide both regulatory robustness and practical certainty for applicants.

Q6: Do you agree that disclosure of on-chain addresses used to receive mining rewards is appropriate, including expectations to update the RA when changes occur? Are there privacy or security concerns that should be addressed?

GDF agrees that disclosure to the Registration Authority (RA) of on-chain addresses used to receive mining rewards can be appropriate within a supervisory context. From a regulatory perspective, such disclosure supports transparency, enables the RA to understand the operational footprint of licensed entities, and may assist in monitoring compliance with licence boundaries, operational activity and AML/CFT expectations.

That said, the manner in which this requirement is implemented will be important to ensure proportionality, operational security and commercial confidentiality.

Operational and Security Considerations

Mining reward addresses are often structured to reflect treasury management, segregation of funds, pooling arrangements, hosting relationships, or security design (e.g., cold storage migration, key rotation practices). Because public blockchain activity is publicly traceable, disclosure of addresses, particularly if widely accessible or insufficiently protected, can reveal:

- Revenue volumes and treasury flows;
- Counterparties and service providers;
- Wallet management structures; and
- Operational scaling decisions.

This creates potential competitive sensitivity and, in certain cases, heightened cybersecurity risk (e.g. targeting of high-balance addresses).

We therefore suggest that:

- Address disclosure should be treated as confidential supervisory information, with explicit confirmation of data protection and secure-handling safeguards.
- The RA clarify that disclosures are for regulatory purposes only and will not be made public.
- Firms be permitted to adopt reasonable address rotation or segregation practices without such changes being interpreted as a supervisory concern.

Ongoing Updates

We recognise the rationale for requiring updates where reward addresses change. However, it would be helpful to clarify that:

- Notification thresholds would apply where changes are material or structural (e.g. migration to a new custody architecture), rather than requiring real-time reporting of routine operational address rotation; and
- Firms may provide disclosure at the level of controlled address clusters, treasury wallets or custody arrangements, rather than individual transient addresses used for technical optimisation.

Beyond confidentiality and rotation flexibility, we would recommend considering a proof-of-control model for relevant reward-flow addresses as an alternative to maintaining exhaustive address registries. Under such an approach, firms could demonstrate control over disclosed address sets (e.g. via cryptographic signing or equivalent validation mechanisms) rather than providing exhaustive and constantly updated inventories.

Similarly, allowing the use of tagged address sets under a documented address-rotation policy would better reflect operational reality. This would permit firms to identify reward-flow categories or wallet clusters governed by internal policy controls, rather than maintaining static address lists that may rapidly become outdated.

If the RA intends to use third-party blockchain analytics providers to monitor disclosed addresses, it would also be helpful to include a short statement clarifying:

- Purpose limitation (i.e. regulatory oversight only);

- Data handling and retention safeguards; and
- Controls governing onward sharing or vendor access.

Given that address management practices may evolve in response to changing cybersecurity risks, flexibility will be important. Overly rigid update requirements could inadvertently discourage the adoption of improved security practices.

In principle, we agree that disclosure of reward addresses to the RA can be appropriate as part of a supervisory framework. However, implementation should:

- Preserve operational security and commercial confidentiality;
- Reflect the technical realities of address rotation and wallet management; and
- Remain proportionate to the scale and risk profile of the mining operation.

A calibrated, principles-based disclosure regime, rather than a highly prescriptive reporting obligation, would best achieve supervisory transparency while safeguarding security and innovation.

Section 4

Q7: Are the proposed general licence conditions clear and proportionate for the sector? Which conditions might benefit from supplemental guidance or examples?

GDF considers the proposed general licence conditions to be broadly clear and proportionate for the sector. The emphasis on ongoing compliance with ADGM legislation, transparency, record-keeping and adherence to licence boundaries reflects sound supervisory practice and is consistent with international approaches to commercial digital asset activities.

That said, we believe that the following areas would also benefit from supplemental guidance or illustrative examples to enhance legal certainty and reduce interpretive risk:

Clarification of "Services to Third Parties"

The Guidance refers to additional expectations where entities offer services to third parties, but the scope of this concept could benefit from further clarification. It would be helpful for the RA to provide examples of what falls within the scope of this concept. For example, clarification would be welcome as to whether this includes:

- Hosted mining arrangements;
- Hashrate leasing or similar contractual structures;

- Mining pool operations; and
- Validator services provided to third parties (where applicable).

Clear examples would reduce the risk of inconsistent interpretation and assist firms that operate hybrid infrastructure models in determining when activities remain within the mining perimeter and when additional regulatory obligations may arise.

Meaning of "Accurate and Comprehensive Business Records"

While the principle is appropriate, additional guidance on what constitutes "accurate and comprehensive business records" in the mining context would be helpful to support consistent supervisory expectations. For example, whether this includes:

- Hardware inventories and lifecycle records;
- Energy procurement documentation;
- Wallet governance policies; and
- Hosting or outsourcing agreements.

It would also be useful to clarify how commercially sensitive operational and technical data will be protected and handled by the RA, particularly where detailed facility, energy or treasury information may have competitive or security implications.

Boundary with FSRA-Regulated Activities

Finally, we recommend explicit clarification of the boundary between crypto mining activities licensed by the RA and any financial services activities regulated by the FSRA. Certain business models (e.g., pooled arrangements, structured hashrate products, validator services with yield-sharing features) could potentially intersect with regulated financial services. Clear perimeter guidance would help firms avoid inadvertent misclassification of activities and ensure appropriate licensing pathways.

Overall, the proposed licence conditions are proportionate and well framed. Supplemental guidance in the areas above would enhance clarity, support compliance planning and further strengthen the operational certainty of the regime.

Q8: Should material outsourcing, changes in overseas footprint, or changes in energy arrangements trigger prior approval or notification? What thresholds would be appropriate?

GDF agrees that certain material changes to a licensed crypto mining entity's operating model, such as significant outsourcing arrangements, changes in overseas footprint, or fundamental shifts in energy sourcing, may warrant regulatory visibility. However, any prior approval or notification framework should be calibrated, proportionate and risk based.

We do not consider that all outsourcing, overseas expansion, or energy adjustments should automatically trigger prior approval. Mining operations are inherently dynamic: hardware hosting arrangements may evolve, facilities may be upgraded, mining pools may change, and energy procurement strategies may change in response to market conditions, efficiency improvements or sustainability objectives. A rigid pre-approval regime could inadvertently constrain operational flexibility without materially enhancing supervisory outcomes.

Material Outsourcing

We would support a notification requirement, rather than prior approval, where outsourcing is material to the core licensed activity. For example, this may include:

- Outsourcing of operational control of mining infrastructure;
- Delegation of wallet management or reward custody; and/or
- Reliance on third-party hosting providers where operational risk materially shifts outside ADGM.

We firmly believe that routine procurement (e.g., hardware suppliers, maintenance contractors) should not fall within this scope. A principles-based "materiality" test, aligned to operational risk, control and accountability, would be preferable to a prescriptive list.

Changes in Overseas Footprint

Where a licensed entity establishes a significant overseas operational presence that is integral to its mining activity (e.g., relocating a substantial portion of hash rate, validator capacity or operational control), notification would be appropriate. This allows the RA to assess supervisory implications, cross-border risk exposure and alignment with licence boundaries.

Minor or temporary overseas arrangements (e.g., pilot deployments, short-term hosting adjustments) should not automatically trigger the need for prior approval, provided they do not alter the fundamental nature of the licensed activity.

Energy Arrangements

Energy sourcing is commercially sensitive and may change frequently in the ordinary course of operations. We do not consider that ordinary changes in energy contracts should require prior approval. However, notification may be appropriate where:

- There is a structural shift in the energy model (e.g., from grid-based supply to co-located generation);
- There are material sustainability implications inconsistent with previously disclosed operational plans; or
- Energy arrangements introduce new regulatory, legal or geopolitical risks.

Thresholds and Calibration

Furthermore, we would suggest that any triggers be based on materiality thresholds linked to:

- Percentage of total operational capacity (e.g., proportion of hash rate or validator capacity affected);
- Changes in operational control or governance responsibility; and/or
- Impact on risk profile, resilience or compliance obligations.

Overall, we believe that a notification-based regime with supervisory discretion for the RA to request further information or impose additional conditions where warranted, rather than one requiring prior approval, would provide the RA with sufficient oversight while preserving operational agility.

We firmly support regulatory visibility over material structural changes, but we recommend a proportionate framework that distinguishes between routine commercial evolution and changes that materially alter the risk profile, governance structure or supervisory perimeter of the licensed entity.

A risk-based notification model, supplemented by prior approval only in clearly defined high-risk scenarios, would strike an appropriate balance between oversight, competitiveness and operational flexibility.

Q9: Which incident types should require immediate notification to the RA, for example cybersecurity breaches, material operational outages, or regulatory actions in other jurisdictions?

GDF agrees that certain material incidents should trigger prompt notification to the RA. However, we recommend that any such framework be clearly risk-based, proportionate to impact and supported by practical guidance to ensure consistent application.

Mining operations, particularly at scale, can experience a range of technical, operational and commercial disruptions, many of which are routine, transient and self-remediating. A notification regime that is overly broad may generate supervisory noise without improving risk oversight. We therefore suggest that the notification triggers be linked to materiality and operational impact, rather than incident category alone.

In principle, immediate notification would be appropriate where an incident:

- Materially disrupts mining operations for a sustained period (e.g. a significant proportion of total hash rate or validator capacity offline beyond a defined threshold);

- Involves a cybersecurity breach that compromises private keys, reward addresses, treasury assets, or critical operational systems;
- Results in unauthorised access, theft or loss of digital assets or reward flows;
- Materially affects business continuity, operational resilience or the entity's ability to operate within licence boundaries; or
- Involves regulatory enforcement, licence suspension or formal investigation in another jurisdiction that may affect the entity's fitness or compliance standing.

Conversely, minor operational interruptions (e.g., short-term power fluctuations, isolated hardware failures or non-material denial-of-service attempts) should not automatically require notification where they are contained, remediated and do not alter the entity's risk profile.

We would recommend that the RA provide:

- Clear materiality thresholds (e.g. percentage of operational capacity impacted, duration of outage, financial impact).
- Guidance on reporting timelines (e.g. immediate notification for critical incidents, periodic reporting for lower-severity events).
- Illustrative examples of best practice incident categorisation and escalation models.

This could take the form of non-binding supervisory guidance aligned with recognised international operational resilience frameworks, allowing firms to map incident severity to reporting obligations in a structured and defensible way.

A calibrated, principles-based notification regime, focused on impact, risk and supervisory relevance, would enhance transparency and resilience without imposing disproportionate reporting burdens or discouraging adaptive operational practices.

Overall, we support incident notification requirements where they are risk-sensitive, clearly defined and operationally workable.

Section 5

Q10: Are the listed supervisory tools adequate? Are there additional tools that would improve oversight, for example standardised data templates or supervisory-technology integrations?

GDF considers the supervisory toolkit described in Section 5 to be comprehensive and broadly appropriate for the oversight of licensed crypto mining entities. The combination of risk-based supervision, off-site monitoring, on-site inspections (including overseas where relevant), third-party verification, thematic reviews and enforcement powers provides the RA with a flexible and proportionate supervisory framework.

In particular, we support the explicit articulation of risk-sensitive supervision. Mining operations vary significantly in scale, complexity and business model, and supervisory intensity should reflect these differences. Larger-scale operators or those offering services to third parties may warrant closer oversight, while smaller proprietary operators may present lower systemic or conduct risk.

Additional Considerations to Enhance Effectiveness

While we support the listed tools, we would also respectfully suggest that supervisory effectiveness could be enhanced through the following measures:

- **Standardised Data Templates (Proportionate and Risk-Based):** The introduction of optional or phased standardised reporting templates, particularly for larger-scale operators, could support consistent supervisory data collection without imposing undue burden. These might include high-level operational metrics (e.g., aggregate hash rate or validator capacity, facility locations, high-level energy sourcing mix and incident

summaries) rather than granular technical telemetry. Templates should remain scalable and aligned with the risk profile of the entity.

- **Supervisory Technology (SupTech) Integration**: Where the RA intends to use third-party blockchain analytics or monitoring tools, clarity around scope and methodology would be beneficial. A structured SupTech approach can enhance supervisory efficiency, particularly for on-chain monitoring and supervisory analytics, but should be implemented in a transparent and proportionate manner. Engagement with industry on tool design and data interpretation would further strengthen supervisory outcomes.
- **Coordinated Cross-Border Engagement:** Given that mining infrastructure and ownership structures may span multiple jurisdictions, mechanisms for regulatory cooperation and information-sharing with relevant overseas authorities (where appropriate) may enhance oversight, particularly in cases involving overseas inspections or regulatory developments in other jurisdictions.
- **Overseas Inspections – Practical Considerations:**
- While we recognise the RA's ability to conduct overseas inspections where relevant, unannounced physical inspections outside ADGM may in practice be difficult to execute due to local legal constraints, third-party hosting arrangements or jurisdictional access limitations. A pragmatic compromise could be for the RA to accept equivalent forms of assurance where physical access is impractical, provided that the RA can obtain effective access to relevant operational, control and assurance information. This could include independent audits, SOC reports or ISO certifications, third-party attestations, or reliance on contractual audit rights embedded in hosting or outsourcing agreements. Such flexibility would preserve supervisory oversight while recognising operational realities.
- **Supervisory Dialogue and Thematic Feedback**: Thematic reviews are a useful tool, particularly in an evolving sector. Publishing anonymised findings, common deficiencies or best practice observations following such reviews would support sector-wide improvement and regulatory certainty.

Overall, we consider the supervisory tools listed to be robust and sufficient. Enhancements, if pursued, should prioritise proportionality, clarity and data standardisation at a level that supports effective oversight without creating unnecessary operational complexity.

A risk-based, technology-enabled supervisory model, combined with transparent expectations and ongoing industry dialogue, will best support ADGM's objective of maintaining high standards while fostering responsible innovation in crypto mining activities.

Q11: Which good-practice indicators should the RA encourage and monitor to support ongoing compliance and sector resilience?

GDF supports the inclusion of clearly articulated good-practice indicators as part of the RA's supervisory dialogue with licensed entities. Well-designed indicators can promote a culture of proactive compliance and operational resilience without imposing rigid or prescriptive requirements.

We would recommend that such indicators remain principles-based, scalable and aligned with operational risk, rather than functioning as de facto mandatory metrics.

In our view, the following categories of good-practice indicators would be appropriate:

- Governance and Oversight
- Operational Resilience, including supply chain and infrastructure Integrity
- Cybersecurity and Key Management Maturity
- Transparency and Record-Keeping
- Sustainability and Energy Transparency

Within these categories, practical indicators could include evidence of mature key-management controls for reward flows or validator signing keys (for example HSM-backed custody, MPC-based signing, or equivalent enterprise controls), infrastructure redundancy and failover capability, concentration risk across pools or hosting providers, and asset or firmware integrity monitoring across deployed hardware. Such indicators would reflect the operational realities of mining and validator infrastructure while remaining adaptable across different operational models.

Importantly, we would recommend that the RA clarify that these indicators are intended as benchmarks for good practice rather than strict compliance thresholds or prescriptive regulatory metrics. The sector would benefit from periodic anonymised thematic feedback highlighting common strengths, weaknesses and emerging risk patterns observed through supervision.

We believe that a principles-based set of indicators, focused on governance quality, operational resilience, infrastructure security and risk management maturity, will better support sector resilience than rigid quantitative thresholds. This approach would also align with ADGM's broader commitment to high standards while preserving flexibility for evolving operational models and technological change.

Overall, we support the encouragement and monitoring of good-practice indicators, provided they remain proportionate, risk-based and adaptable to different scales of operation.

Section 6

Q12: Are the disclosure expectations for overseas operations appropriate in scope and detail? Are there additional data points that would be useful, for example energy mix in host jurisdictions, pool operator details, or sanctions-screening results?

GDF recognises the rationale for requiring ADGM-registered headquarters to provide visibility over global mining operations that they manage, direct or oversee. Where strategic direction, governance control or treasury management is exercised from ADGM, it is reasonable for the RA to have sufficient information to assess consolidated operational and financial risk.

While overall we are supportive of the objective of the proposed requirements, we would encourage careful calibration to ensure that disclosure expectations remain proportionate to the degree of control exercised from ADGM and to the materiality of the overseas operations within the broader group structure.

Territorial and Proportionality Considerations

We would respectfully note that much of the information contemplated relates to activities occurring outside ADGM's legal perimeter and may already be subject to local regulatory frameworks. While consolidated risk assessment is legitimate, we would caution that disclosure obligations should not inadvertently evolve into expectations that extend beyond ADGM's supervisory nexus for operational activities that are more appropriately overseen by host jurisdictions.

We therefore suggest that:

- Disclosure should be clearly tied to governance nexus (i.e., where decision-making authority, treasury control or risk management oversight is exercised from ADGM).
- Reporting should focus on material overseas operations rather than minor or incidental exposures within the global infrastructure footprint.
- The RA rely on high-level attestations or consolidated risk summaries where appropriate, rather than granular operational reporting on overseas operations.

Additional Data Points

With respect to potential additional data points such as energy mix, pool operator details or sanctions-screening outcomes:

- Energy mix may be relevant where it materially affects operational risk, sustainability representations or jurisdictional exposure to energy supply constraints, but should not become a routine mandatory metric.
- Pool operator concentration risk may warrant disclosure where operational dependency or revenue concentration is significant.
- Confirmation of sanctions and jurisdictional risk assessments may be appropriate at a policy or governance level, rather than requiring detailed screening outputs or transactional data.

In our view, the most effective approach would be a principles-based consolidated supervision model centred on governance accountability and risk management oversight, rather than exhaustive operational reporting across global footprints.

Overall, we support the objective of risk visibility but recommend that the framework be expressly grounded in proportionality, materiality and respect for territorial regulatory boundaries. This will help maintain ADGM's high standards without inadvertently creating duplicative or extraterritorial reporting burdens.

Q13: Do you agree with due-diligence expectations on host jurisdictions and partners? Are there specific criteria, benchmarks, or public sources that should be referenced?

GDF agrees that Crypto Mining Entities headquartered in ADGM should conduct appropriate due diligence on host jurisdictions and key overseas partners. Where governance control, capital allocation or strategic oversight is exercised from ADGM, it is reasonable for the RA to expect that firms understand and manage cross-border regulatory, operational and integrity risks arising from those activities.

However, we note as with our response to the previous questions that such expectations should remain proportionate, risk-based and clearly anchored to the extent of governance or operational control exercised from ADGM. We believe that due-diligence requirements should not result in inadvertent expectations that ADGM-registered entities exercise supervisory control over overseas operations that are subject to host-jurisdiction regulation. We would suggest that due-diligence requirements be calibrated according to:

- The materiality of the overseas operation to the group as a whole;
- The level of governance, operational control or decision-making exercised from ADGM;
- The regulatory risk profile of the host jurisdiction; and

- The criticality of the third-party partner to core mining or infrastructure operations.

Higher-risk jurisdictions or structurally significant outsourcing arrangements may justify deeper assessment and enhanced monitoring, while low-risk or minority exposures should not trigger disproportionate documentation requirements.

Reference Points and Benchmarks

If the RA wishes to provide greater clarity, it may be helpful to reference widely recognised public benchmarks and risk indicators used in global risk assessment frameworks, such as:

- FATF mutual evaluation reports and high-risk jurisdiction lists;
- World Bank governance indicators or similar macro risk metrics;
- Public sanctions regimes (e.g., UN, UAE, OFAC, EU); or
- International cybersecurity or operational resilience standards where relevant.

Referencing established global sources would promote consistency and avoid the need for the RA to define standalone risk taxonomies.

Balance and Territorial Considerations

Importantly, we believe that expectations should focus on ensuring that ADGM-registered entities can demonstrate structured and documented risk assessment processes, rather than requiring them to guarantee outcomes in overseas jurisdictions. The emphasis should be on governance quality, documented analysis and appropriate risk mitigation, rather than exhaustive operational control over foreign-regulated entities.

Overall, we support due-diligence expectations that are structured, principles-based and aligned with international benchmarks, provided they remain proportionate to the degree of supervisory nexus with ADGM and do not extend beyond ADGM's legitimate regulatory perimeter and supervisory mandate.