SUBMITTED VIA SURVEYS

To whom it may concern,

Re: FCA CP25/25 on the Application of the FCA Handbook for Regulated Cryptoasset Activities Chapters 1-5

About Global Digital Finance (GDF) and Crypto Council for Innovation

GDF and CCI are the two leading global members' associations representing firms delivering crypto and digital assets solutions. Our members span the digital asset ecosystem and include the leading global crypto exchanges, stablecoin issuers, digital asset Financial Market Infrastructure providers, innovators, and investors operating in the global financial services sector.

Together, our members share the goal of encouraging the responsible global regulation of crypto and digital assets to unlock economic potential, improve lives, foster financial inclusion, protect security, and disrupt illicit activity.

We believe that achieving these goals requires informed, evidence-based policy decisions realised through collaborative engagement between regulators and industry. It also requires recognition of the transformative potential of crypto and digital assets, as well as new technologies, in improving and empowering the lives of global consumers.

We support and encourage a comprehensive UK digital asset regulatory approach which is robust, proportionate, and pro innovation. Appropriate regulatory guardrails are crucial to ensure the continued growth of the UK ecosystem, to further attract the predominantly global industry, and to realising the goal of making the UK a digital finance hub.

The input to this response has been curated through a series of member discussions, industry engagement, and roundtables, and both GDF and CCI are grateful to their members who have taken part.

As always, we remain 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 – Executive Director – GDF

Laura Navaratnam - UK Policy Lead, CCI

Response to the Public Consultations: Executive Summary

Global Digital Finance (GDF), jointly with the Crypto Council for Innovation (CCI), convened their joint membership to analyse the Financial Conduct Authority's Consultation Paper CP25/25 on the Application of the FCA Handbook for Regulated Cryptoasset Activities. The following is in response to the questions set out in chapters 1-5.

GDF and CCI welcome the FCA's proactive approach in seeking to establish a clear and proportionate regulatory framework for qualifying cryptoasset activities in the UK. We strongly support the FCA's objectives of ensuring market integrity, consumer protection, and operational resilience, while fostering innovation in digital assets and financial services.

This draft response brings together feedback from our members and industry participants with the aim of providing constructive input into the consultation process. In particular, the response highlights areas where further clarification, proportionality, or additional guidance may be beneficial to support the effective implementation of the FCA's proposals.

We are broadly supportive of the FCA's proposal to treat qualifying cryptoasset activities as designated investment business for the purposes of Handbook application. This approach ensures regulatory coherence while maintaining legal clarity that cryptoassets themselves are not re-characterised as specified investments under the RAO. We recommend explicit signposting for qualifying stablecoins as a defined subset of cryptoassets with payment and settlement functions, ensuring prudential and redemption rules are applied appropriately and proportionately.

GDF and CCI support the extension of the FCA's High-Level Standards to cryptoasset firms, provided that alignment remains outcomes-based rather than process-driven. The framework should account for the operational realities of decentralised systems and distributed-ledger infrastructure, focusing on accountability for matters within a firm's control. In line with this, we welcome the FCA's technology-neutral stance but encourage early supervisory statements and illustrative guidance at authorisation stage to promote consistent interpretation across firms.

We agree with the proposed application of the SUP rules, excluding SUP 16, and the SYSC framework to cryptoasset firms, while urging a phased and proportionate approach. Further guidance will be needed on audit and skilled-person reviews, data collection, record-keeping of on-chain information, and intra-group governance to ensure operational feasibility. Likewise, applying SYSC 4–10 and 18 to crypto firms should recognise group structures, decentralised dependencies, and the need for flexibility in governance and outsourcing expectations.

We support applying the Senior Managers and Certification Regime to cryptoasset firms but emphasise the importance of proportionality and clarity for global group structures. Guidance should explain how reasonable steps are interpreted where accountability interacts with

decentralised technologies. We request that the FCA reconsiders the proposal to prevent crypto custodians and stablecoin issuers from designating a non-SMF individual as CASS oversight as technical expertise, not hierarchy, should determine fitness for this role.

We welcome the proposed extension of the operational-resilience framework (SYSC 15A) and agree that use of permissionless DLTs should not be treated as outsourcing. Resilience standards must be flexible enough to reflect distributed architectures, network-level dependencies, and collaborative testing approaches. The FCA should continue aligning expectations with its Critical Third Parties regime and provide clarity on how firms should map and test decentralised dependencies.

We support the application of the existing financial-crime framework, provided it remains technology-neutral and recognises blockchain analytics, “know-your-transaction” tools, and on-chain provenance as valid controls. Alignment with the JMLSG Guidance and FATF Recommendation 15 will be key to ensuring coherent implementation across cross-border business models.

GDF and CCI also endorse the FCA’s plans to apply the ESG Sourcebook to cryptoasset firms in a phased and proportionate manner. Given limited availability of reliable data on blockchain energy use and other sustainability metrics, early guidance should allow qualitative or best-effort reporting and coordination with evolving international standards before quantitative disclosures become mandatory.

Across all chapters, we encourage the FCA to continue engaging closely with industry as firms progress through authorisation and supervision. Early guidance, case studies, and practical examples, particularly relating to on-chain data, incident reporting, and consumer-duty outcomes, will ensure consistent interpretation, proportionality, and a smoother transition into regulation.

Response to consultation questions

Chapter 1-5

Question 1: Do you agree that new cryptoasset activities defined in the SI (and as described as 'qualifying cryptoasset activities' in draft FCA Handbook rules) should fall under the category of 'designated investment business' for the purposes of applying relevant sections of the Handbook??

Yes, we support the FCA's proposal to categorise qualifying cryptoasset activities as 'designated investment business'. This approach ensures regulatory coherence across the financial services framework and appropriately recognises the comparable risks and functions of qualifying cryptoasset activities to traditional investment activities.

It may, however, be helpful for the FCA to clarify that the DIB classification operates primarily as a regulatory conduit, a mechanism for applying relevant Handbook modules, rather than as a recharacterisation of qualifying cryptoassets themselves as specified investments under the RAO. This distinction will help prevent interpretive uncertainty regarding the legal nature of the assets and preserve the intended scope of existing regulatory definitions.

We also suggest that the FCA explicitly signpost the treatment of qualifying stablecoins as a defined sub-set of cryptoassets with payment and settlement functions, rather than investment characteristics. In this context, the DIB framework should be applied in a way that preserves their prudential and redemption-related focus, avoiding any implication that such instruments are being treated as investment products.

The FCA should also focus DIB-related obligations on activities with a material UK nexus, consistent with the Financial Services and Markets Act 2023 competitiveness and growth objective. This would ensure proportionate oversight targeted to genuine UK market risks while supporting the international competitiveness of the UK as a jurisdiction for responsible digital assets innovation.

We note that the effect of broadening the category of designated investment business will result in many of the COBs provisions applying to qualifying cryptoasset activities. We recognise that these considerations have not yet been dealt with in full so underscore the importance of proportionate application in due course with sector specific guidance where needed.

Question 2: Do you agree with our proposal for applying High Level Standards to cryptoasset firms in a similar way they apply to traditional finance?

Yes, we support the FCA's proposal to extend the High Level Standards to authorised cryptoasset firms in a way that is consistent with the approach applied to traditional financial

services. As GDF and CCI have long advocated, aligning qualifying cryptoasset regulation with existing financial services frameworks where appropriate promotes consistency for firms seeking authorisation and trust for consumers engaging with regulated products.

We also recommend emphasising outcome-based alignment rather than process replication. Furthermore, we believe that High Level Standards should be applied proportionately, reflecting the operational realities of cryptoasset business models such as distributed infrastructure, validator dependencies, and the use of open-source components, while ensuring the same consumer and market integrity outcomes as in traditional finance.

In particular, accountability under SYSC should attach to decisions and risks that are within a firm's control, rather than to decentralised or open-protocol functions that operate independently of the firm. This distinction is essential to ensure that responsibility and oversight obligations remain meaningful and enforceable in a blockchain environment where certain technical or governance outcomes cannot be directed by any single entity.

In this context, achieving Consumer Duty outcomes through the existing conduct modules (COBS, PROD, CASS, and DISP) rather than through an extension of PRIN 2A would maintain consistency with the approach outlined in Chapter 6 of the consultation.

Additionally, we believe that early supervisory engagement through the authorisation process and thematic work will also be key to ensuring interpretive consistency as the regime is implemented across diverse business models. Proactive engagement and early guidance will help firms understand how these standards are expected to apply in practice and support coherent supervision as the sector integrates into the wider regulatory perimeter.

Applying standards such as the Principles for Businesses and the General Provisions will help embed strong governance, accountability, and conduct expectations across the crypto sector, while signalling that authorised cryptoasset firms are held to comparable standards of integrity and prudence. We particularly welcome the FCA's intent to do so in a proportionate and technology-neutral manner, recognising the operational and structural differences between crypto-native firms and traditional intermediaries.

Whilst we support this for authorised cryptoasset firms, the proposal to extend the FCA's Principles for Businesses (PRIN) to stablecoin issuers in respect of all token holders presents significant practical challenges. Stablecoin issuers generally do not have direct contractual relationships with all holders, as tokens can be freely transferred across secondary markets and through peer-to-peer transactions beyond the issuer's control or visibility. This makes it impossible for issuers to identify, interact with, or influence the experience of all holders, raising uncertainty over how obligations particularly those under Principles 6 to 9 could reasonably be met. Applying PRIN in this way risks misaligning accountability and creating expectations that cannot be effectively fulfilled or supervised in practice. We therefore encourage the FCA to

adopt a similar approach to the proposed application of PRIN to CATPs, and disapply PRIN 6 and 9 to stablecoin issuers.

Question 3:Do you agree with our proposed application of the existing SUP rules (except SUP 16) to cryptoasset firms?

GDF & CCI broadly support the FCA's proposal to apply the existing SUP rules (with the exception of SUP 16) to firms conducting regulated qualifying cryptoasset activities. Applying the supervisory framework consistently across financial services, including the crypto asset sector, will help ensure continuity, accountability, and effective oversight as the market matures.

However, we encourage the FCA to consider several practical adjustments and areas where further guidance may be warranted to ensure proportionality and operational feasibility in the early stages of the regime's implementation.

First, audit and skilled-person requirements may require calibration. Given the relative youth of the cryptoasset industry, there remains a limited pool of audit and assurance teams with demonstrable expertise in digital-asset custody, on-chain attestations, and valuation methodologies. The FCA should consider a proportionate, transitional approach to auditor expectations and promote collaboration between audit firms, supervisors, and industry to develop appropriate standards.

Second, information-gathering and skilled-person reviews under SUP 1–SUP 5 may need clarification to ensure that data requests reflect the distinctive structure of distributed-ledger systems and take account of nuances which may exist across on- and off-chain records. Guidance on what constitutes "reasonable" expectations in these contexts would aid firms' readiness.

Third, variation of permission (VOP) and modification by consent processes should reflect the rapid pace of product innovation in the sector. Firms may frequently update their models (for example, by adding staking, tokenisation, or new custody arrangements), and a proportionate, agile variation process, aligned to the changes proposed by HMT in their recent review of authorisation and VOP timelines, would support compliance across the ecosystem without unduly constraining innovation.

Fourth, the FCA may wish to provide additional clarity on record-keeping and notification obligations, including expectations around the retention and reconciliation of on-chain data, operational resilience reporting, and senior-management notification triggers for technology incidents or smart-contract failures. We encourage the FCA to consider how FCA reporting portals and technologies may be updated to have greater interoperability with on-chain data in the future.

Fifth, guidance on how group and cross-border mechanics under SUP 13 and 13A will apply in practice would also be valuable. Firms would benefit from clarification on when notification and

data obligations extend to non-UK affiliates and how duplication can be avoided with existing group governance, supervisory coordination, and MLR reporting frameworks.

We continue to support the decision to exclude SUP 16 at this stage. However, we recommend that, once firms' data-collection capabilities are better understood, the FCA work with industry to co-develop a bespoke, risk-based reporting pack focused on safeguarding, operational resilience, and key market indicators relevant to cryptoasset business models.

We also recognise that some of the more detailed expectations around competence, expertise, and capacity, including for auditors, assurance providers, and senior managers, may be addressed in the forthcoming FCA work on training and competence assessments. Nevertheless, we believe it is important to flag these interdependencies here, as supervisory expectations under SUP will depend in part on the availability of suitably qualified professionals across the sector.

Overall, GDF & CCI support the proposed application of SUP but recommend that the FCA adopt a phased and proportionate supervisory approach, supported by tailored guidance in the areas of audit assurance, information-gathering, variation procedures, and record-keeping, to reflect the evolving maturity of the cryptoasset ecosystem.

Question 4: Do you agree with our proposal to require cryptoasset firms to follow the existing requirements in SYSC 1, 4 – 7, 9 – 10, and 18 in a similar way to existing FCA-regulated firms (or existing DIBs)?

GDF and CCI broadly support the FCA's proposal to apply the existing SYSC framework to authorised cryptoasset firms. We agree that extending these core systems and controls requirements will strengthen governance standards, enhance market integrity, and provide regulatory consistency across the financial-services landscape.

That said, we encourage the FCA to apply these requirements in a proportionate and risk-sensitive manner that reflects the relative maturity and diversity of the UK's cryptoasset sector.

In particular:

- **Governance and oversight:** SYSC 4–6 requirements should recognise that many cryptoasset firms are smaller, technology-native, or operating as subsidiaries within global groups. The FCA should confirm that simplified governance arrangements, appropriate to a firm's size, complexity, and risk profile, may still satisfy the underlying principles of effective oversight and accountability. This would help ensure that governance expectations focus on accountability within the authorised firm's control, rather than mandating legacy organisational forms that may not align with digital-native business models.

- **Outsourcing and third-party arrangements:** The FCA should clarify how SYSC 8 expectations interact with decentralised or blockchain-native service providers. For example, in instances where node operators or protocol developers are not contractually bound service providers, firms may be unable to meet traditional due-diligence or substitution requirements. Additional guidance on what constitutes "material outsourcing" in these contexts would be valuable.

  We also recommend that the FCA recognise intra-group outsourcing arrangements where group-wide governance, controls, and risk management frameworks provide equivalent assurance. This would help avoid unintended duplication of contractual documentation and oversight processes at the UK-entity level, while maintaining effective accountability within the group's overall supervisory framework.

- **Risk management and conflicts of interest:** Novel risks may arise where firms may simultaneously act as validator nodes, token issuers, or liquidity providers. Illustrative examples of good practice, co-developed with industry, under SYSC 7 and 10, particularly for managing token holdings or validator rewards that overlap with client interests, would support consistent application across firms. GDF and CCI would be happy to support in the development of such examples.

We note that the FCA intends to issue a separate consultation on training and competence. Nevertheless, as noted in our response to the previous question we consider it important to flag the strong interdependence between competence standards and SYSC outcomes. The effectiveness of SYSC requirements, especially in governance, compliance, and risk management, will rely on the availability of staff with the necessary expertise in distributed-ledger technology, custody models, and digital-asset market structure.

Drawing on our previous work on knowledge and competence under MiCA, we highlight several factors for the FCA's consideration as it develops the forthcoming framework:

- **Limited existing qualifications:** There is currently no standardised set of recognised degrees or certifications specific to blockchain or digital-asset markets, meaning firms may struggle to demonstrate competence through traditional credentialing routes.

- **Need for flexible pathways:** Many staff develop expertise through technical or self-directed learning rather than formal courses. The FCA should recognise modular, experiential, and industry-led learning as valid means of demonstrating competence.

- **Transitional arrangements:** Given the nascent state of professional education in this field, firms will require transitional provisions and clear grandfathering for existing personnel.

- **Industry collaboration:** The FCA could support public-private initiatives to develop accredited digital-asset training programmes, building a pipeline of qualified professionals over time.

As operational resilience matters are addressed later in the consultation, we will also provide more detailed comments later in our response related to those proposals.

Overall, GDF and CCI supports the proposed application of SYSC 1, 4–7, 9–10, and 18 to cryptoasset firms, while encouraging the FCA to ensure that proportionality, practical implementation, and competence development are considered in tandem as part of the broader regime design.

Question 5: Do you agree with our proposal to apply the existing SM&CR regime to cryptoasset firms, taking into account various parallel consultations on the broader SM&CR regime to ensure consistency? If not, please explain why.

We are broadly supportive of the FCA's proposals to apply the SM&CR to cryptoasset firms. A clear and proportionate accountability framework will help promote strong governance, responsible decision-making, and public confidence as the sector transitions into regulation.

That said, proportionality will be key to ensuring that the regime works effectively across the diverse range of crypto business models. We encourage the FCA to provide further sector-specific guidance to ensure consistent and practical application across firms with varying structures, functions, and global footprints.

We note the broader changes to the regime which were proposed in CP25/21. Of these proposals we underscore the following:

SMF7 – Group entity senior manager at solo-regulated firms.

- Given the global nature of many cryptoasset businesses, it is common for key individuals with significant influence to sit within group entities overseas. Clear expectations on how these roles will be assessed and approved will be essential to ensure operational clarity and avoid duplicative or conflicting governance requirements.

The Duty of Responsibility.

- While we recognise this duty is enshrined in legislation, we believe it will be important for the FCA to articulate how "reasonable steps" should be interpreted in the context of crypto firms. Given the unique operational structures of many crypto businesses, including decentralised elements, open-source dependencies, and validator or protocol-level components, there will be practical challenges in determining the boundaries of accountability. The FCA's guidance should acknowledge these nuances and provide illustrative examples where possible.

- We also encourage the FCA to explicitly confirm that references to Consumer Duty within this context remain consistent with the approach set out in Chapter 6 of the consultation. In line with this, we support regulated firms being expected to achieve equivalent consumer outcomes through the existing conduct modules, such as COBS, PROD, CASS, and DISP, rather than through any wholesale extension of PRIN 2A. Maintaining this outcome-based alignment will promote proportionality and avoid duplicative supervisory expectations.

The Certification Regime.

- We also note the broader reforms to the certification regime currently being considered. We support the FCA's intention to streamline certification and re-certification processes and reduce duplication across roles and functions. A simplified and proportionate certification framework will be particularly valuable for cryptoasset firms, which often operate with leaner compliance teams and agile organisational structures that differ from traditional financial institutions. Ensuring that certification requirements are aligned to genuine risk and responsibility, rather than simply mirroring legacy models, will help maintain appropriate accountability without creating unnecessary administrative burden.
- Certification and senior-manager assessments should also encompass relevant technical expertise. For example, this could include blockchain engineering, custody architecture, and cybersecurity to ensure that accountability extends to technology-native functions and that individuals responsible for critical technical decisions are appropriately competent and certified.
- Given the evolving nature of the crypto sector and the diversity of firm types entering regulation, we would welcome further engagement with industry once the final approach is confirmed. This will help ensure that the framework is calibrated appropriately to the operational realities of crypto firms, including cross-border governance arrangements, decentralised infrastructure components, and the presence of global group structures. Ongoing dialogue with industry at this stage would also allow the FCA to identify areas where additional guidance or flexibility might be needed to ensure that certification remains both effective and proportionate.

With regards to the proposals in 3.50, we do not support the proposal to prevent cryptoasset custodians and stablecoin issuers from certifying individuals under the CASS oversight function. The exemption that allows firms to designate a non-SMF individual to perform this role was originally introduced to provide flexibility where the function requires deep technical and operational expertise. This rationale applies equally, and arguably even more strongly, to cryptoasset firms, where operations often involve global teams, cross-border infrastructure, and streamlined resourcing. The key consideration should be that the individual responsible has sufficient knowledge and expertise to discharge the oversight function effectively, rather than their formal position within the senior management structure. Removing this flexibility risks the

function being allocated to a Senior Manager without the necessary technical competence, which could undermine rather than enhance client asset protection.

We appreciate that the certification regime is currently under broader review and that changes to it may have implications for this exemption. However, we maintain that the CASS oversight function, whether within traditional or cryptoasset firms, must ultimately be performed by an appropriately qualified individual, not assigned purely on the basis of hierarchy.

Finally, we note the FCA's statement (page 28) that it does not expect any crypto firms to be "limited scope" at the gateway. We do not believe this assumption will hold true in all cases. For instance, certain service companies such as trading system providers or other firms authorised solely for "making arrangements" may appropriately fall within the limited-scope definition. We would welcome clarification from the FCA that such firms can indeed be categorised as limited scope where this reflects their business model and risk profile. Furthermore, we also note that the interaction with forthcoming SM&CR reforms introducing proportional adjustments for smaller or less complex firms should also extend to cryptoasset entities, ensuring that procedural obligations do not create unnecessary administrative burden where they offer limited governance value.

Question 6: Do you agree with the proposed categorisation for enhanced cryptoasset firms, such as the threshold for allowing cryptoasset custodian firms to qualify as enhanced? Should we consider other ways to categorise cryptoassets firms as enhanced?

Overall, GDF and CCI broadly support the FCA's proposal to apply the enhanced-firm categorisation to cryptoasset entities where scale, risk, or systemic importance justify additional governance and oversight requirements. However, we encourage the FCA to refine the criteria to ensure proportionality and effective risk capture.

Rather than relying primarily on traditional metrics such as headcount or revenue, we would encourage the FCA to weight the thresholds more toward functional risk, for example, the scale of custody operations, the concentration of client assets in omnibus wallets, third-party and technology dependencies, and interconnections with critical market infrastructure. We believe that these characteristics more accurately reflect where enhanced governance and resilience obligations would add supervisory value.

We also suggest exploring a modular enhanced approach, whereby enhanced expectations apply specifically to high-risk functions such as safeguarding, custody, or operational resilience, without automatically imposing the full suite of enhanced-firm requirements across the entire business. We also believe that this would ensure that regulatory intensity is directed toward areas of genuine systemic or consumer risk while maintaining proportionality for smaller or less complex cryptoasset firms.

Question 7: Do you agree with our proposal to extend the application of SYSC 15A to cover all cryptoasset firms, including FSMA-authorised firms carrying out qualifying cryptoasset activities? If not, please explain why.

GDF & CCI broadly support the extension of SYSC 15A (the Operational Resilience Framework) to cryptoasset firms. Embedding resilience standards early in the regime is vital to ensuring continuity of critical services, maintaining market confidence, and strengthening supervisory trust in this rapidly developing sector.

That said, we believe that the FCA should consider certain nuances in how operational resilience principles, particularly scenario testing, mapping, and dependency management, are applied in a digital-native environment. Furthermore, the FCA's operational resilience framework should be flexible enough to accommodate diverse DLT governance models, as applying rules built for centralised intermediaries risks conceptual and practical inconsistencies. We expand on these recommendations below:

Scenario testing and impact tolerances

- Scenario testing in the cryptoasset sector will necessarily diverge from traditional models. First, we would note that key disruption scenarios may stem from events external to the firm's direct control, such as validator or oracle failures, blockchain network congestion, protocol upgrades, or custody-bridge vulnerabilities. The FCA should clarify whether, and to what extent, firms are expected to design scenarios around such externalities, and what constitutes a "reasonable" boundary for testing where service continuity depends on third-party or decentralised infrastructure.
- For DLT-based business models, recovery and continuity planning may depend more on governance coordination (for example, protocol rollbacks or multisig interventions) than on internal system redundancies. The FCA may wish to provide illustrative guidance on how firms can evidence preparedness and testing for these decentralised dependencies.

Third-party and critical-service dependencies

- Many cryptoasset firms rely on external providers (which may be traditional or novel) such as custody technology vendors, cloud infrastructure, liquidity venues, and node operators, for key operational functions. Mapping and managing these dependencies will be essential to identifying "important business services". We therefore encourage the FCA to clarify how SYSC 15A interacts with its existing outsourcing existing Critical Third Parties (CTP) regime, allowing firms to rely on established group-level frameworks for oversight and continuity where appropriate, so as to avoid unnecessary duplication of controls at the UK entity level. Furthermore, we also believe clarity would be beneficial on whether cryptoasset firms will be expected to treat certain protocol or infrastructure providers as "material dependencies" for resilience-planning purposes.

- We also believe that FCA should ensure alignment with the Critical Third Parties framework, providing clear guidance on when reliance on designated CTPs will be deemed to meet oversight and assurance expectations under SYSC 15A. This alignment would help firms manage dependencies consistently and avoid duplicative supervisory obligations across overlapping resilience regimes.
- It would also be helpful for the FCA to clarify that "important business services" should capture activities where the firm has direct operational responsibility, such as custody, onboarding, and trading systems, rather than network-level or protocol processes outside the firm's control. Testing methodologies and impact tolerances should similarly reflect crypto-specific disruption scenarios, including chain reorganisations, validator downtime, or bridge and oracle failures.
- Additionally, where certain protocol or infrastructure providers are deemed material dependencies, the FCA could consider novel approaches to resilience planning in a digital-native environment, including collaborative testing and scenario sharing between firms and infrastructure partners.

Testing methods and proportionality

- Building on the previous points, we would also note that given the relative immaturity of resilience-testing tools and the limited availability of DLT-specific expertise, the FCA should allow proportionate flexibility in how firms meet the scenario-testing requirement, for example, by recognising table-top exercises, simulation environments, or collaborative testing with infrastructure partners during early implementation phases. Traditional CBEST testing may need to be reframed or adjusted for digital-native environments in order for firms to meet expectations, but also for systems to be appropriately tested.

Incident response and communications

- Finally, as cryptoasset firms may in some cases operate predominately online and often across multiple jurisdictions, material incidents may propagate rapidly and require real-time communication across platforms. The FCA may wish to provide clarity on thresholds for material incident notifications under SYSC 15A and ensure alignment with its existing incident reporting expectations for operational disruptions and cyber incidents.

Distinguishing Public Networks from Centralised Service Models

- The FCA's proposals should avoid conflating the use of distributed ledger infrastructure with the existence of a centralised service provider. Public DLT networks are open, shared infrastructures maintained by diverse participants rather than as single legal entities capable of contractual or outsourcing relationships. Firms building on such

networks cannot exercise control through conventional means and should instead be expected to evidence sound governance and risk management practices appropriate to their dependencies, such as testing, contingency planning, and transparent disclosure, rather than contractual oversight of entities that do not exist in a traditional sense.

- Accordingly, it is important that the FCA's framework continues to focus on functional accountability; that is, on how a regulated firm uses or depends upon a network, rather than on network typologies. While we do not propose that the FCA strictly defines categories such as "public," "private," "permissioned," or "permissionless," we emphasise that open public networks provide transparency, auditability, and resilience benefits that private systems do not. Recognising these characteristics within the operational resilience and outsourcing frameworks would ensure proportionate treatment of firms using public DLT infrastructure, without implying regulatory oversight of the protocols themselves.
- Finally, the FCA should ensure that expectations around organisational and risk management controls should be applied in a technology-neutral manner, focusing on how firms manage their operational dependencies and consumer outcomes, rather than on the architectural design of the networks on which they build.

Overall, GDF and CCI support the extension of SYSC 15A to cryptoasset firms but recommend that the FCA adopt a phased, proportionate approach, supplemented by guidance specific to distributed-ledger-based operations, third-party dependencies, and scenario testing methodologies. This would help ensure operational resilience standards are robust yet achievable, while reflecting the structural realities of digital-native financial infrastructure.

Question 8: Do you agree with our proposal that the use of permissionless DLTs by cryptoasset firms should not be treated as an outsourcing arrangement? If not, please explain why.

Yes, GDF and CCI strongly agree with the FCA's proposal that the use of permissionless distributed-ledger technology (DLT) by cryptoasset firms should *not* be treated as an outsourcing arrangement. This proposal appropriately recognises that open, decentralised networks do not operate under a single accountable entity and therefore cannot be managed, contracted, or supervised in the same way as a traditional third-party service provider.

Permissionless DLTs clearly operate as open, decentralised infrastructures rather than discrete, controllable service providers. As GDF highlighted in its 2023 response to IOSCO's consultation on decentralised finance, such systems are credibly neutral and sufficiently decentralised such that there is no meaningful "service relationship" between a firm and the underlying protocol. Applying traditional outsourcing rules, designed for bilateral, contract-based relationships, would therefore be technologically inappropriate and risk introducing obligations that firms cannot fulfil.

We would note the following key considerations as the FCA continues to build out its DLT guidance:

- **Structural distinction:** Public DLTs are not bespoke third-party services. They lack the hallmarks of an outsourcing arrangement, such as contractual oversight, service-level agreements, audit rights, and substitution or termination rights.
- **Accountability:** The regulated firm remains responsible for how it *uses* the network (for example, deploying smart contracts, or managing custody processes) but not for the operation of the infrastructure itself. This distinction preserves accountability for regulated activities without conflating public infrastructure with vendor relationships.
- **Proportionality and innovation:** Treating public DLTs as outsourcing could stifle innovation and disincentivise the use of open networks that provide transparency, resilience, and interoperability benefits. Recognising them instead as public infrastructure supports the FCA's objective of a proportionate, technology-neutral regime.
- **Boundary clarity:** GDF recommends that the FCA provide short guidance as part of its final policy statement to delineate:
    - the use of open, public networks; and
    - the use of intermediated infrastructure providers (for example, commercial node or API services), which may constitute outsourcing *if and where* contractual control exists.

This will ensure firms can confidently distinguish between infrastructure reliance and outsourced service provision.

In conclusion, GDF and CCI strongly support the FCA's position. Recognising permissionless DLTs as neutral public infrastructure, rather than outsourced services, appropriately reflects their technical characteristics, maintains accountability for regulated activities, and aligns with GDF's prior recommendations on proportionate regulation of decentralised finance.

Question 9: Do you agree with our proposal to require cryptoasset firms to follow the same financial crime framework as FSMA authorised firms? If not, please explain why.

We agree with the proposal to apply the existing financial crime framework to cryptoasset firms. Applying consistent standards across sectors will help strengthen market integrity and build consumer confidence.

We however encourage the FCA to adopt a technology-neutral approach that recognises the role of blockchain analytics and "know-your-transaction" (KYT) tools as valid financial crime controls under SYSC. These capabilities often provide equivalent or superior transparency to traditional monitoring techniques. The FCA should also clarify the relationship between

FSMA-based and MLR-based obligations to avoid duplicative requirements and ensure firms have clarity on regulatory precedence and equivalence.

Given the cross-border nature of the cryptoasset market, the FCA may also wish to provide guidance on managing counterparties or customers where conventional identity verification methods are not feasible, including appropriate reliance on technological mitigations and on-chain provenance tools.

Furthermore, we believe that the FCA should ensure consistency with the JMLSG Guidance (Part 1 Chapter 5 and Part 2 Sector 22), explicitly recognising blockchain analytics, digital ID verification, and proof-of-origin tools as proportionate mitigations where counterparties cannot be identified by conventional means. This alignment would help firms apply risk-based controls with confidence while maintaining coherence across existing AML and CTF frameworks.

Finally, we support continued alignment with FATF Recommendation 15 and related information-sharing initiatives to reduce fragmentation, support international supervisory cooperation, and enable effective cross-border enforcement.

Question 10: Do you agree with the guidance set out in this document, and can you outline any areas where you think our approach could be clearer or better tailored to the specific risks and business models in the cryptoasset sector?

Overall, GDF and CCI welcome the FCA's efforts to provide early guidance to support the implementation of the new cryptoasset regime. Clear supervisory expectations will be essential to ensuring consistent interpretation and proportionate application across a diverse and rapidly evolving sector.

We encourage the FCA to continue refining its guidance through ongoing engagement with industry, particularly as firms progress through authorisation and supervisory interaction begins. This will help identify areas where additional clarification or good-practice examples could further improve consistency and reduce interpretive uncertainty.

We also recommend that the FCA explicitly cross-reference HM Treasury's Statutory Instrument definitions of qualifying cryptoasset and qualifying stablecoin to anchor perimeter interpretation and reduce potential ambiguity around hybrid or multi-function tokens. Aligning terminology across legislative and supervisory instruments will help firms clearly determine whether specific assets or activities fall within scope and minimise regulatory uncertainty where tokens have overlapping payment, settlement, or investment characteristics.

Finally, we also believe it would be helpful for the FCA to include illustrative use-cases demonstrating how existing requirements and expectations should apply in practice, for example, incident-reporting thresholds, mapping on-chain transparency to record-keeping obligations, and consumer-understanding prompts relating to custody, transaction finality, or fee disclosures.

Including anonymised examples from early authorisations would further help illustrate the proportionate application of obligations and provide firms with practical reference points as the regime embeds. Providing such examples would help ensure consistent application across firms and promote better alignment between supervisory intent and operational implementation.

Overall, we welcome the FCA's proportionate and pragmatic approach to guidance and encourage continued collaboration with industry to ensure that expectations evolve in step with market and technological developments.

Question 11: Are there any emerging digital and cyber security industry practices or measures which we should consider when supporting cryptoasset firms complying with operational resilience and related requirements? Please elaborate.

GDF and CCI welcome the FCA's focus on cyber and operational resilience within the cryptoasset regime. The unique technology stack underpinning cryptoassets, spanning private-key management, smart contracts, decentralised infrastructure, and cross-chain interactions, creates nuanced and unique risk profiles that may not be fully captured by traditional frameworks.

We encourage the FCA to recognise and, where appropriate, reference illustrative (rather than prescriptive) examples of leading digital-asset security and resilience practices in its guidance. These could include multi-party computation (MPC) or threshold-signature schemes, hardware-backed multi-factor authentication, software bill of materials (SBOM) and code-signing requirements, bug-bounty and responsible-disclosure programmes, crypto-specific red-team scenarios, and clear expectations for maintaining a Resilience Reference Pack. Highlighting such practices would help firms demonstrate that they meet operational-resilience outcomes without relying on rigid or outdated templates.

We also encourage the FCA to continue liaising with the National Cyber Security Centre (NCSC) and industry groups developing security baselines for digital-asset custody and smart-contract management, to ensure a coherent and proportionate approach across regulatory and technical domains.

Additionally, as discussed throughout our response we encourage the FCA to recognise decentralisation, open-source transparency, and architectural diversity as emerging best practices in cyber-resilience for the cryptoasset sector. In distributed ledger systems, resilience is achieved not only through traditional perimeter defences or contingency planning, but also through the design of the network itself, which distributes authority, validation, and data storage across multiple independent actors. This structure mitigates single points of failure, reduces systemic dependencies, and enhances continuity even under stress conditions such as node compromise, infrastructure outages, or targeted attacks.

Many modern blockchain and DLT networks also integrate with established cybersecurity and risk management tools, including penetration testing frameworks, continuous vulnerability scanning, and SIEM systems, enabling regulated firms to incorporate them into their own operational resilience and incident response programmes. Open source governance further enhances transparency and accountability by allowing independent review of codebases and security practices.

Recognising these features as complementary to, rather than substitutes for, traditional cybersecurity controls would allow the FCA to promote proportionate, forward-looking resilience standards tailored to digital-native infrastructures. Such an approach would help ensure that operational resilience expectations evolve in step with technological innovation, supporting the FCA's broader objectives of market integrity, operational continuity, and technology neutrality, while reinforcing the UK's competitiveness as a hub for responsible digital-finance innovation.

Question 12: Do you agree with our proposal to apply the ESG Sourcebook to cryptoasset firms?

GDF and CCI support the FCA's proposal to apply the ESG Sourcebook to cryptoasset firms. Embedding ESG standards will help strengthen governance, transparency, and accountability in a sector where sustainability claims and operational models are rapidly evolving.

That said, several crypto-specific factors may warrant an adjusted proportionate application as well as future sector-specific guidance. First, reliable environmental or social data, particularly on blockchain energy use or validator activity, remains limited, and the FCA should permit flexibility in early disclosures while industry methodologies mature. Second, the risk of misleading sustainability claims in areas such as "green tokens," "carbon-neutral chains," or "sustainable staking" underscores the importance of clear examples of good practice under the anti-greenwashing rule. Finally, smaller or technology-led firms may need phased implementation to ensure reporting remains proportionate to their scale and risk profile.

We also recommend that the FCA adopt a phased and proportionate approach to applying the ESG Sourcebook. Priority should be given to activities with measurable environmental externalities, such as mining, validation, or custody infrastructure, while allowing best-efforts estimates and qualitative disclosures for service-based firms until data quality and methodologies improve. We also would note that coordination of measurement approaches with emerging international standards, including the ISSB, IOSCO, and ESRS frameworks, will help ensure consistency and comparability before mandating detailed quantitative reporting.

In addition, we would caution that the FCA should avoid introducing premature disclosure obligations that could lead to inconsistent or misleading metrics given current data limitations. The regime could be revisited once reliable and widely adopted measurement and assurance practices for blockchain energy use and other environmental impacts are more consistently

available, ensuring that ESG reporting meaningfully reflects underlying performance rather than forcing early standardisation on immature data.

Overall, GDF supports the FCA's approach and encourages continued engagement to ensure ESG expectations evolve in step with improved data quality, standardisation, and market maturity across the cryptoasset ecosystem.