Subject: EMA response to FCA Consultation Paper - Application of FCA Handbook for Regulated Cryptoasset Activities (Chapters 1-5)

Date: 12.11.2025

Chapter 1 – Overview and Scope

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?

EMA response:
We broadly agree that bringing qualifying cryptoasset activities within the scope of the Handbook is appropriate. However, the framework must be carefully delineated so that it captures genuinely financial services activities - such as issuance, custody, and trading - while excluding purely technological or infrastructure-based functions that do not involve client assets or regulated intermediation.

Without clear boundaries, there is a material risk that the definition of "designated investment business" could unintentionally capture software developers, infrastructure providers, or validators who play no role in client-facing or custodial functions.

The FCA should therefore accompany this definition with detailed perimeter guidance, including examples distinguishing regulated activities from neutral infrastructure or technology services. This clarity will ensure firms can confidently assess authorisation requirements and avoid regulatory overreach that could constrain innovation.

Chapter 2 – High Level Standards and supervision

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?

EMA response:
EMA supports the application of consistent high-level regulatory principles, such as integrity, transparency, and fair treatment of customers. However, these principles should be interpreted in a way that reflects the structural and operational differences between crypto markets and traditional finance.

Directly mirroring legacy frameworks risks imposing rules designed for intermediated, issuer-led products onto decentralised or open-market systems. We therefore recommend that the FCA adopt an outcome-based approach, preserving the intent of high-level standards while recognising that the methods for achieving them - such as on-chain transparency, smart contract automation, or open-access audits - will differ materially from those used in traditional financial institutions.

Question 3:

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

EMA response:
While supervisory and reporting obligations under SUP can apply, the regime must be proportionately calibrated to the diversity of crypto business models. For example, smaller specialist providers or firms offering technology-enabled services should not face the same data and reporting burdens as large multi-asset trading platforms.

We recommend that the FCA develop crypto-specific SUP guidance and templates, including proportionate reporting frequencies, streamlined event notifications, and clarification on how traditional reporting categories (e.g., product sales, customer complaints) translate into crypto contexts. SUP 16 should be revisited to ensure reporting obligations are designed for digital-asset data rather than inherited from MiFID-era systems.

Chapter 3 – Governance, Systems and Controls

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 the same way as existing FCA-regulated firms (or existing DIBs)?

EMA response:
While robust systems and controls are essential for cryptoasset firms, the FCA should recognise that the technical controls and governance mechanisms used in this sector differ significantly from those in traditional finance.

Applying SYSC provisions in full - without modification - could create compliance gaps or force firms into ineffective processes. For example, crypto custody risk can be managed through multi-signature access, cold storage segregation, and smart-contract controls, which are not captured by conventional CASS or SYSC frameworks.

Therefore, while we support the principle of applying SYSC, it is essential that this be supplemented by crypto-specific guidance confirming that blockchain-native risk management, key-control procedures, and resilience frameworks are accepted as equivalent. This ensures consistent outcomes without enforcing outdated operational models.

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.

EMA response:
We do not support a direct application of the existing SM&CR framework to all cryptoasset firms in its current form. While accountability and governance are important, the regime should be tailored to the scale, complexity, and structure of crypto businesses.

Many crypto firms are lean, technology-driven, and decentralised. Imposing the full SM&CR model used by major banks would be disproportionate and administratively onerous, especially where firms already maintain robust executive accountability structures. We therefore recommend a tiered accountability model, similar to the limited-scope approach, where SM&CR requirements scale according to firm size and risk.

The FCA should also clarify how accountability applies where operational control is shared across entities (e.g., global exchanges or decentralised governance structures) to avoid uncertainty or duplication.

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?

EMA response:
We do not support broad classification of cryptoasset firms as "enhanced" unless they are systemic in size, complexity, or market impact. Enhanced supervision should apply only where a firm's activities present material risks to UK market integrity or consumer protection - such as large custodians holding substantial client assets or platforms facilitating high trading volumes.

Applying enhanced status too widely would impose disproportionate costs and create a two-tier market where only the largest firms can meet the associated obligations. The FCA should adopt objective, risk-based criteria (e.g., quantitative thresholds for assets under custody or systemic interlinkages) and review these periodically to ensure that firms are categorised appropriately as their operations evolve.

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.

EMA response:
Yes, subject to proportionate application. Operational resilience is critical for safeguarding clients and maintaining confidence, but the FCA must acknowledge the unique dependencies of crypto businesses on public or decentralised networks.

Incident reporting should focus on material operational disruptions affecting consumers or market access. The FCA should clarify that not all on-chain events - such as network delays, protocol upgrades, or validator issues - require regulatory reporting unless they directly affect a firm's ability to meet obligations. This ensures oversight remains meaningful and avoids overwhelming firms or the FCA with immaterial reports.

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.

EMA response:
We agree. Treating the use of public or permissionless DLTs as outsourcing would be conceptually incorrect and operationally impossible. These networks function as shared infrastructure rather than third-party suppliers, and firms have no contractual control over their participants.

EMA welcomes the FCA's clarification and suggests that firms instead be expected to identify, monitor, and disclose protocol-related risks - for example, governance concentration or code vulnerabilities - within their risk frameworks, rather than treating them as outsourcing dependencies. This approach maintains accountability without constraining use of open networks that underpin innovation and market development.

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.

EMA response:
We support maintaining strong financial-crime controls but do not agree that crypto firms should simply follow the same framework as FSMA-authorised firms. The risk typologies, transaction data, and mitigation tools in crypto markets differ significantly from traditional finance.

Rather than mirroring legacy AML/CTF processes, the FCA should explicitly recognise the effectiveness of blockchain-analytics, wallet-risk scoring, on-chain transaction monitoring, and sanctions-screening technologies already used by the sector.

These methods offer transparency and traceability advantages that traditional systems lack. We therefore recommend that the FCA adapt its Financial Crime Guide to formally incorporate these crypto-specific tools as acceptable (and often superior) risk-mitigation mechanisms, ensuring consistency while leveraging the strengths of blockchain transparency.

Chapter 4 – Operational Resilience and Financial Crime

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?

EMA response:
We broadly support the guidance but believe several areas need further clarification to ensure effective implementation. In particular:

- The interaction between MLR registration and FSMA authorisation should be clearly defined to avoid duplicative compliance expectations.
- Guidance on cross-border operations and equivalence with international regimes (e.g., MiCA, MAS, NYDFS) should be expanded.
- The FCA should publish examples of compliant operational-resilience arrangements, illustrating how crypto-native firms can meet standards without replicating legacy infrastructure.

A clearer, practical framework supported by case studies and FAQs would ensure consistent interpretation across firms and supervisory teams.

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.

EMA response:
Yes. The FCA should incorporate recognition of blockchain-native security frameworks and emerging practices that are already standard across the sector. These include:

- Multi-signature and threshold key management, which mitigates single-point-of-failure risks in custody.
- Cold and warm wallet segregation, with automated withdrawal controls and audit trails.
- Smart-contract audits and formal verification to reduce exploitable code vulnerabilities.

- Independent penetration testing and bug-bounty programmes, which are integral to security assurance in decentralised systems.

Operational resilience standards should focus on capabilities and outcomes - maintaining asset security and service continuity - rather than prescriptive processes.

Chapter 5 – Business Standards

Question 12:

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

EMA response:
Only where relevant. While ESG considerations are increasingly important, blanket application of the ESG Sourcebook would not be appropriate for all crypto firms. Many operate in non-lending, non-investment, or infrastructure capacities where ESG disclosures offer limited value to consumers.

Where cryptoasset firms engage in activities with measurable environmental or social impact - such as stablecoin issuance, staking, or tokenisation - they should report ESG data that is proportionate and meaningful, focusing on governance and sustainability of operations. The approach should allow to draw as much as possible on cooperative arrangements and processes ensuring effective and fully consistent reporting.

However, for infrastructure providers, wallet services, or pure technology entities, ESG reporting should remain voluntary and principles-based.

Any mandatory framework should recognise technological diversity (e.g., proof-of-stake versus proof-of-work) and avoid penalising specific consensus mechanisms. The FCA should coordinate with international initiatives (OECD, IOSCO, MiCA) to ensure consistency and avoid duplicative or conflicting metrics.