FINANCIAL CONDUCT AUTHORITY

Finalised Guidance

Guidance on Cryptoasset Operational Resilience

FG26/6

Published: 30 June 2026

1 Introduction

1.1 Operational resilience is fundamental to the integrity and stability of financial services. The cryptoasset sector relies heavily on digital technology to deliver services and support the systems and infrastructure to conduct their activities.

1.2 Under the new cryptoasset regime, we are applying our existing operational resilience framework to cryptoasset firms. This includes the following requirements and standards:

- SYSC 4 (General Risk Management Requirements)
- SYSC 7 (Risk Control)
- SYSC 8 (Outsourcing)
- SYSC 15A (Operational Resilience Requirements)

1.3 This guidance is designed to help firms implement our operational resilience requirements (SYSC 15A), with reference to our outsourcing provisions under SYSC 8, under the cryptoasset regime. To ensure this guidance is relevant for cryptoasset firms, we focus on:

a. Cryptoasset-specific operational and technological risks that, due to the unique characteristics of cryptoassets, may happen more often in the cryptoasset sector than in traditional financial services, presenting distinct challenges for firms.

b. Using example cryptoasset business models to demonstrate how operational resilience requirements can apply in practice within regulated cryptoasset activities, giving firms examples of how they can build resilience.

1.4 Please consider separate forthcoming non-Handbook guidance on operational resilience for distributed ledger technology (DLT) use. This guidance is aimed at supporting firms in managing DLT-specific operational and technological risks, using example firms to demonstrate how operational resilience requirements can apply in practice in permissionless and permissioned DLT use cases.

2 Cryptoasset-specific operational and technological risks

2.1 While many operational and technological risks are common in both traditional financial firms and cryptoasset firms, the unique characteristics of cryptoassets introduce specific challenges. The table below highlights some of these. This is not a complete list and is intended to provide an initial overview. We will explore each risk further throughout the guidance to help firms build operational resilience.

2.2 Firms should remain aware of emerging technologies that may affect their operational resilience, such as advances in artificial intelligence (AI), quantum computing, and other technologies that may introduce new vulnerabilities and dependencies or change existing risk profiles.

Code vulnerabilities	Use of code such as smart contracts can potentially make cryptoasset firms vulnerable to hacks if they do not adequately test, review and (where applicable) update the underlying code on an ongoing basis.
Private key security risks	Private key security risk refers to the risk of unauthorised access to private keys, which may result in the loss or theft of cryptoassets. For example, cyberattacks may expose private keys, enabling the attacker to steal consumers' cryptoassets. These attacks can occur if wallets storing private keys are not adequately protected, for example, due to weak access controls.
Validator risks	Validator risk arises when cryptoasset firms rely on validators (e.g. for staking) without conducting appropriate due diligence or ensuring adequate controls. Misconduct or operational failures by validators, such as double signing, can lead to slashing penalties (having a portion of staked assets forfeited) and loss of staked assets for the firm and its clients.
Service disruptions	Service disruption risks involve disruptions to services or underlying technologies (such as distributed ledger technology) which prevent consumers from accessing or transacting with their cryptoassets when needed. This can leave consumers unable to sell during price volatility or make time-sensitive payments, leading to financial loss.

Cyber risks and cyber security

2.3 In addition to crypto-native risks, cyber risks also present a unique challenge for the cryptoasset sector. As part of maintaining their operational resilience, firms should also consider how to identify and address cyber risks.

2.4 The FCA, the PRA and the Bank of England have set out good cyber response and recovery practices observed across systemic firms and financial market infrastructures. Cryptoasset firms should review these practices to strengthen their operational resilience. Firms should also read the latest annual CBEST thematics published by the FCA, the PRA and the Bank of England and consider embedding the findings into their cyber strategies.

Example firms

2.5 We use 5 fictional example firms in this document to illustrate how our operational resilience requirements might apply to different types of firms conducting or supporting regulated cryptoasset activities. While these examples are illustrative, the risks and scenarios described may be applicable across all example firms. These examples do not cover all scenarios or business models and there will be instances where firms might implement our operational resilience requirements using a different approach. As noted above, we will be covering DLT-specific example firms through separate guidance.

2.6 Each example firm is assumed to have a UK-registered office. As per SYSC 15A.1.4[R], SYSC 15A does not apply to a firm which has its registered office (or, if it has no registered office, its head office) outside the UK. In-scope UK firms that operate overseas branches may want to voluntarily apply some or all of the requirements to those branches to support a consistent approach across their operations.

Firm A: Qualifying Stablecoin Issuer

Firm A is a qualifying stablecoin issuer that issues a stablecoin referenced to a fiat currency. The firm's business model involves offering the stablecoin to the public, undertaking the redemption and maintaining the value of the stablecoin (e.g. managing the backing assets). The issuer has created their stablecoin on multiple permissionless DLTs.

The firm has embedded freeze functionality in the stablecoin's on-chain contract logic which can be used if stablecoins are stolen or linked to illicit activity, helping to improve security and general compliance against their regulatory requirements.

Firm B: Qualifying Cryptoasset Trading Platform

Firm B operates a cryptoasset trading platform in the UK providing services to retail and institutional clients. Retail clients and institutional clients receive direct access to advanced trading services via dedicated interfaces and APIs, enabling automated and algorithmic trading. Firm B maintains robust order-matching systems, liquidity pools and secure omnibus cryptoasset wallets.

As part of their Customer Due Diligence (CDD) processes, Firm B outsources client identity verification to a specialised third-party provider, maintaining clear service level agreements. Firm B retains internal oversight of outsourced services,

Firm B: Qualifying Cryptoasset Trading Platform

regularly evaluates provider performance and ensures the arrangement supports operational continuity and regulatory compliance.

Firm C: Qualifying Cryptoasset Staking

Firm C offers custodial staking services to retail and institutional clients across multiple proof-of-stake (PoS) blockchain networks. Clients place their cryptoassets into Firm C's platform, where the firm handles all aspects of the staking process on their behalf.

Rather than running its own validator nodes (systems that validate transactions and secure the blockchain in return for rewards), Firm C outsources the operation of validator nodes, delegating clients' cryptoassets to a network of third-party validator operators under formal outsourcing arrangements. These third parties manage the infrastructure and participate in network consensus on Firm C's behalf. As a custodial service, Firm C also stores private keys associated with the staked cryptoassets, implementing controls to maintain secure storage and controlled access for clients.

Firm D: Cryptoasset Custody

Firm D provides cryptoasset custody services to retail and institutional clients, safeguarding a broad range of cryptoassets across multiple blockchain networks. Clients deposit cryptoassets with Firm D to hold or store the means of access to the cryptoasset, i.e. to protect the private key used to access the cryptoasset. It operates a hybrid storage architecture that combines cold and hot wallet infrastructure.

Cold wallets are used for long-term storage. Hot wallets are used to support real-time transactional activity. Firm D uses multi-party computation (MPC) to split and secure cryptographic keys across multiple systems, reducing the risk of compromise. In addition to custody, Firm D offers clients real-time reporting tools and maintains recovery plans for loss of access or security breaches. Clients engage solely through Firm D's platform, which acts as their single point of access, while the firm manages all interactions with underlying blockchain networks on their behalf.

Firm E: Intermediary Firm Arranging Deals

Firm E is a multi-asset intermediary which arranges deals in qualifying cryptoassets for retail and institutional clients. Clients use Firm E's arranger platform to place buy/sell orders, which Firm E then routes to UK-authorised third-party execution venues.

When transmitting orders for clients, Firm E checks prices across multiple execution venues to meet best execution requirements.

Firm E also relies on a third-party on/off ramp partner to facilitate deposits and withdrawals of cryptoassets and fiat currency.

3 Operational resilience framework guidance

3.1 Firms in scope of SYSC and engaged in cryptoasset activities should apply the principles in SYSC 15A, such as when identifying important business services, setting impact tolerances, mapping dependencies and conducting scenario testing. In line with SYSC 15A.3.1[R], firms must have in place sound, effective and comprehensive strategies, processes and systems.

3.2 The table below illustrates sound operational risk management practices and should inform each stage of our operational resilience framework:

Key focus area	***Expectations for cryptoasset firms***
Cyber and Technology Resilience	Firms should maintain robust and proportionate cyber and IT controls to ensure their systems which support cryptoasset-related services are resilient. This includes managing risks to system availability, data integrity, third-party dependencies and using recognised international cyber security standards and relevant best practices.
Safeguarding Cryptographic Keys and Infrastructure	Where firms hold or store the means of access to the cryptoasset (e.g. private keys), including any supporting infrastructure to provide this service (e.g. smart contracts or validator nodes), they should establish secure and well-defined processes. These processes should address the management of private key loss, unauthorised system access, and general service disruptions. Examples of emerging practices across the sector include multi-party computation (MPC), multisignature and threshold key management, Hardware Security Modules (HSMs), zero-trust defence architecture, distributed storage, cold and warm wallet segregation, and cryptographic audit logs. To be fully effective, these tools should be used in a way that avoids centralising risks. We expect firms to adopt and maintain high technical standards to safeguard both private keys and the resilience of the underlying infrastructure as outlined above.
Continuity and Disruption Planning	Firms should create, test, and regularly update plans to maintain or restore critical services during disruptions. Scenarios should reflect cryptoasset activities that a firm carries out and the underlying infrastructure to support the service (e.g. smart contract failure, failure in the technology to support stablecoin reconciliation processes and validator outages). Targeted vulnerability scans and penetration tests should be carried out and proven to identify and address risks, including testing security and access systems to address cyber risks. Firms should also be able to evidence monitoring and logging systems.

3.3 In line with SYSC 15A.3.2[R], the strategies, processes and systems that firms have in place to comply with SYSC 15A obligations must be comprehensive and proportionate to the nature, scale and complexity of the firm's activities.

3.4 This guidance should be read alongside our final Policy Statements on our cryptoasset regime, and PS21/3 (operational resilience), which complements this

guidance by covering broader, non-crypto considerations, as well as our upcoming non-handbook guidance on operational resilience for DLT use.

4 Outsourcing expectations for cryptoasset firms

4.1 When reading the guidance below, cryptoasset firms in scope of SYSC should also consider our outsourcing requirements under SYSC 8. The Handbook defines outsourcing for SYSC 8 as 'an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself.'

4.2 As such, firms should read each section of this guidance with SYSC 8 in mind and, as per SYSC 8.1.7[R] apply appropriate skill, care, and diligence to outsourced arrangements. They should consider the nature, scale and complexity of those arrangements in the context of their operational resilience planning. This includes arrangements with both traditional service providers and other technology providers where relevant.

4.3 Additionally, as per SYSC 8.1.12[G], a firm should notify the FCA when it intends to rely on a third party for the performance of operational functions which are critical or important for the performance of relevant services. In the context of cryptoassets, a critical or important outsourcing arrangement could include, but is not limited to:

- Custody infrastructure (e.g. MPC and HSM providers)
- Validator services (e.g. third-party node operators)
- Cloud service providers hosting trading platforms, custody systems, or settlement infrastructure
- Security-critical services (e.g. transaction signing infrastructure)

4.4 Recognising the challenges of applying the above definition to permissionless DLTs, the use of permissionless DLTs should not be treated as an outsourcing arrangement under SYSC 8.1.1[R].

4.5 Nevertheless, we expect cryptoasset firms to evaluate their internal operational controls for permissionless DLTs, following the operational resilience framework in SYSC 15A and the guidance below. Ultimately, firms remain responsible for maintaining their own operational resilience.

5 Identifying important business services

5.1 SYSC 15A.2.1[R] states that all firms within scope of SYSC 15A must clearly identify their important business services to ensure they can remain operationally resilient. As outlined in the previous chapter, this requirement also applies to cryptoasset firms in scope of SYSC, along with all subsequent requirements set out below. As per

SYSC 15A.2.2[R] firms must keep their assessments of important business services under review.

5.2 As defined in the FCA Handbook glossary, an important business service means a service provided by a firm, or by another person on behalf of the firm, to one or more clients of the firm which, if disrupted, could:

- cause intolerable levels of harm to any one or more of the firm's clients, or;
- pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of financial markets.

Factors to consider when identifying important business services

5.3 Cryptoasset firms may rely on third parties to deliver their important business services. Firms must ensure these services are appropriately identified, mapped and tested in line with our operational resilience requirements. Additionally, firms still remain fully responsible for following our requirements in cases where firms have limited control over the third-party (e.g. permissionless DLTs).

5.4 Where a cryptoasset firm performs multiple activities (e.g. a cryptoasset principal dealer that also offers custody and staking services), the delivery of these activities is likely to be underpinned by multiple important business services. Firms should clearly identify each of these as separate important business services.

5.5 Cryptoasset firms often primarily serve retail customers, some of whom may be particularly vulnerable to service disruptions, especially where outages prevent transactions from being executed or disrupt essential services (e.g. where stablecoins are used for payments).

5.6 We are also seeing cryptoasset services becoming more closely interconnected with traditional financial markets (e.g. traditional custodians safeguarding stablecoin backing assets), increasing the potential for wider market contagion if disruptions occur. Firms should adopt a holistic approach when identifying their important business services, taking into account the full, non-exhaustive list of relevant factors set out in SYSC 15A.2.4[G].

5.7 Correctly identifying these important business services is the foundation for complying with our operational resilience framework and ensuring operational risks are appropriately accounted for and managed.

How our example firms might identify important business services

Firm A: Qualifying Stablecoin Issuer
Firm A, the stablecoin issuer, identifies the redemption of its fiat-referenced stablecoin as one of its important business services. Holders rely on Firm A to convert stablecoins back into money and for the firm to place a payment order to return the money to the client. A disruption to this service could prevent a holder from accessing the redemption amount. Additionally, given the role of stablecoins in potentially enabling payments and trading activity across cryptoasset markets, a public disruption could also undermine confidence in the stablecoin and contribute to broader market instability.

Firm B: Qualifying Cryptoasset Trading Platform

Firm B, the cryptoasset trading platform, identifies the matching and execution of orders as one of its important business services. Market participants rely on the platform to execute trades efficiently and at market prices.

A failure in this service could disrupt market liquidity, impair price formation and cause financial losses for clients. Prolonged disruption may also undermine confidence in the platform, damage its reputation, and contribute to instability across other firms connected to the platform, causing disruption or loss of access for clients.

Firm C: Qualifying Cryptoasset Staking

Firm C identifies the operation of validator nodes, managed by third-party technology providers, as one of its important business services. Clients rely on Firm C to stake their cryptoassets and earn rewards through these validator nodes.

If the third-party providers fail to run the nodes properly, Firm C may be unable to perform key functions such as distributing rewards and could face slashing penalties. This could cause intolerable harm via financial loss to consumers and affect Firm C's ability to operate its business.

Firm D: Cryptoasset Custody

Firm D, the cryptoasset custody provider, identifies providing and managing secure custody solutions as one of its important business services. Clients depend on Firm D to safeguard their cryptoassets and for continued access to them.

A disruption could prevent clients from accessing their assets when needed, leading to financial loss, reduced liquidity and greater exposure to market volatility. This may also affect other firms that rely on timely asset transfers or settlement, increasing the risk of wider disruption.

Firm E: Intermediary Firm Arranging Deals

Firm E, the intermediary, identifies the receipt and transmission of orders for execution as one of its important business services. Clients rely on Firm E to arrange trades quickly and provide access to a wide range of assets.

A disruption to this service could disrupt market liquidity and execution quality, and cause financial losses for clients.

6 Setting impact tolerances

6.1 Once a firm has identified their important business services, SYSC 15A.2.5[R] requires it to clearly define impact tolerances for each of its important business services. Impact tolerances represent the maximum level of disruption to an important business service a firm judges acceptable before further disruption causes

intolerable harm to any one or more of the firm's clients (e.g. through financial losses, delayed rewards, lost transactions), or poses a risk to the soundness, stability or resilience of the UK financial system or orderly operation of the financial markets.

6.2 Cryptoasset firms in scope of SYSC must also ensure they can maintain their impact tolerance for each of their important business services if there is a severe but plausible operational disruption, in accordance with SYSC 15A.2.9[R].

Factors to consider when setting impact tolerances

6.3 In-scope cryptoasset firms should establish a clear scale, measured by a length of time and any other relevant metrics (including but not limited to transaction throughput or confirmation latency thresholds, error rates for critical smart contracts and transaction success rates), that determines how long an important business service can be disrupted before the firm exceeds its impact tolerance. Firms should calibrate these tolerances to reflect the nature of their services, client base, and associated risks. Firms should consider the non-exhaustive list of relevant factors in SYSC 15A.2.7[G], when setting their impact tolerances.

6.4 As set out in SYSC 15A.2.8[G], when setting impact tolerances, cryptoasset firms should consider how demand for each of their important business services may fluctuate, particularly during periods of heightened market activity. For example, cryptoasset markets operate 24/7 and can experience sudden spikes in trading volumes. Firms should ensure their impact tolerances are appropriately calibrated to reflect these fluctuations, including periods of peak demand, to maintain operational resilience under the most severe but plausible conditions. Examples of appropriately calibrating impact tolerances might include shortening maximum downtimes for trading engines or maximum tolerable access disruptions to hot wallets during periods of high volatility. Firms should also consider how to appropriately calibrate to avoid market contagion, given the interconnectedness of services between traditional financial and cryptoasset markets.

6.5 As cryptoasset firms often operate multiple services, there may be instances where their service suffers multiple disruptions within a short timeframe. While firms should consider the potential aggregate impact of disruption to multiple important business services when setting impact tolerances, nevertheless, firms are expected to set their impact tolerances with reference to a single disruption event, rather than an aggregate of multiple disruptions. This approach is essential to ensure impact tolerances remain a precise and reliable metric for the maximum level of disruption that can be tolerated.

6.6 Firms must monitor their impact tolerances on an ongoing basis and, where these are breached, ensure that appropriate business continuity and contingency plans are in place to manage and mitigate harm.

7 Use of third-parties and multiple disruptions when setting impact tolerances

7.1 As noted in the previous section, when a firm uses a third-party provider in the delivery of an important business service, they should work effectively with the third-party to set impact tolerances. A firm should ensure the provider remains within those tolerances and monitors its performance against those tolerances on an ongoing basis. Where that is not possible (for example, when there is no contractual relationship), the responsibility for setting and remaining within impact tolerances remains with the firm.

7.2 Setting accurate impact tolerances ensures firms can effectively prevent, adapt, respond to and recover from operational disruptions.

Resuming a degraded service

7.3 A degraded service means a partially functioning service operating below full capacity. Firms should have clear plans and criteria for resuming a degraded service during disruptions. Firms should consider running a degraded service when the risks of not doing so are greater. In line with SYSC 15A.2.10[G], firms should generally not resume a service if this would put the firm in breach of another regulatory obligation, or result in increased risk to its clients, the UK financial system or the orderly operation of the financial markets.

7.4 Given the complexities of cryptoasset business models, firms are encouraged to carefully assess and test when, and how, resuming a degraded service may reduce intolerable harm while balancing broader operational and security considerations. We provide examples below:

- **A cryptoasset trading platform suffers a disruption following a cyberattack.** To minimise harm to clients and maintain market confidence, it makes a strategic decision to partially restore functionality in a degraded mode. While full trading is not available, users can still access account balances and make limited withdrawals.

  The firm determines that this limited functionality reduces the risk of consumer harm without compromising the platform's security. Throughout the incident, the firm communicates transparently with clients, clearly setting expectations about service limitations while it works to safely restore full operations.

- **Following a critical incident affecting its infrastructure provider, a cryptoasset custody firm loses access to part of its key management system**, temporarily halting withdrawal processing. Rather than rushing to resume full service, the firm conducts an impact assessment and determines that partial restoration can support clients without compromising asset security.

  The firm enables read-only access to customer wallets and transaction histories, helping users verify asset holdings and account activity. Withdrawals remain paused to avoid introducing further risk while forensic checks are completed. By restoring this limited functionality, the firm reduces uncertainty and supports customer confidence during the disruption.

How our example firms might set impact tolerances

Firm A: Qualifying Stablecoin Issuer

To set an impact tolerance, Firm A considers the potential harm if there is a failure in the underlying DLT. It identifies that client harm is the most relevant, given the number of consumers affected and their reliance on the service to redeem their stablecoins to money.

Using redemption rate forecasts, Firm A concludes that being unable to process redemptions over an 8-hour period, due to system outage, would be outside the firm's impact tolerance. A delay to processing redemption requests within this period would lead to significant disruption and therefore an intolerable risk of consumer harm.

Firm B: Qualifying Cryptoasset Trading Platform

Firm B has identified that disruption to its cryptoasset trading platform could lead to considerable client harm. Clients rely heavily on uninterrupted access to the platform to manage their cryptoasset exposure effectively. Recognising the critical need for ongoing service availability, Firm B considers the maximum tolerable period for disruption to its trading platform, including the order-matching system, should be set somewhere between 1-24 hours (depending on the scale of the disruption).

This timeframe reflects the rapid nature of cryptoasset market transactions, reducing the risk of financial losses and disruption of liquidity.

Firm C: Qualifying Cryptoasset Staking

To set an impact tolerance, Firm C works closely with its third-party providers to understand potential harm. Firm C identifies client harm as the main risk, given clients' reliance on staking rewards and the possibility of financial loss if rewards are missed or penalties occur.

If a validator goes offline, rewards stop and do not accrue until service resumes. Prolonged downtime can also lead to penalties such as slashing. Firm C reviews validator performance, reward timing and disruption durations that could cause these outcomes.

Based on this, Firm C sets a time-based impact tolerance, such as a maximum disruption of 24–48 hours, after which client harm would be intolerable. Firm C maintains regular communication with its providers to ensure the impact tolerance can be met during disruptions.

Firm D: Cryptoasset Custody

To set an impact tolerance, Firm D considers the potential harm to clients if they cannot access their wallets. Clients depend on continuous access to both hot wallets, for transactional activity, and cold wallets, for secure long-term storage. A disruption could result in missed trading opportunities, liquidity constraints or financial loss during periods of market volatility.

Firm D analyses typical wallet usage patterns, including transaction volumes and withdrawal frequencies. It also considers the potential for disruptions to affect multiple services that depend on custody, amplifying the overall impact. Using a time-based metric, Firm D sets its impact tolerance at 4 hours, subject to firm-specific factors such as systems and technologies used.

Firm E: Intermediary Firm Arranging Deals

To set an impact tolerance, Firm E considers the potential harm to clients if it is unable to receive and transmit orders for execution. It identifies that disruption and delays can lead to increased client harm due to missed trading opportunities for consumers and financial loss during periods of market volatility. Firm E also recognises the time sensitive nature of cryptoasset market transactions and the critical need for ongoing service availability and access to liquidity.

Based on this, Firm E sets a time-based impact tolerance after which client harm would be intolerable, at somewhere between 1-24 hours. When setting the timeframe, Firm E considers availability of alternative intermediaries in the market during the period of disruption.

8 Mapping exercises

8.1 Under SYSC 15A.4.1[R], cryptoasset firms must identify and document the people, processes, technology, facilities and information necessary to deliver each of their important business services. This mapping must be sufficiently detailed to support effective impact tolerance testing and help firms understand their vulnerabilities and remedy these as appropriate.

8.2 For further information on the definitions of people, processes, technology, facilities and information, please refer to PS21/3.

Examples of cryptoasset-specific vulnerabilities identified via mapping

8.3 Given the nature of cryptoasset business models – including features such as decentralisation, third-party reliance and evolving technologies – firms should pay particular attention to the unique risks and vulnerabilities involved when mapping their technologies:

- Unavailability of critical third-party services such as DLT providers (especially in the case of permissionless DLTs), including business continuity plans and off-chain controls.
- Significant technology disruptions affecting cryptoasset transaction processing (e.g. smart contract failures or blockchain outages).
- Loss or reduced provision of critical infrastructure supporting cryptoasset services (e.g. failure of primary trading platform infrastructure).

8.4 Cryptoasset firms remain fully responsible for accurately mapping any relationships with third parties. Where a firm relies on third-party providers – such as custodians, validators, off-chain oracle services, or fiat on/off-ramp partners – it must be able to identify and understand any vulnerabilities in those arrangements, whether they lie directly with the third party or further along the service chain. If firms are unable to obtain sufficient information from the third party to satisfy themselves that they can operate within tolerance, then they should review and where necessary change their arrangements.

8.5 However, third parties may lack direct contractual agreements, such as some permissionless DLTs. In these cases, firms must strengthen internal controls and monitoring to identify and address vulnerabilities beyond traditional oversight and remedy as appropriate. This may involve enhanced transaction monitoring across on-chain and off-chain activities, stress-testing node connectivity, and performing regular independent audits of smart contracts.

8.6 In sum, firms should map vulnerabilities under their contractual control, vulnerabilities arising from external network risks, and the mitigations in place for each. Where infrastructure is beyond a firm's control, the expectation is that the firm has appropriate remedies in place such as contingency plans in the event of a disruption (factored in via its business continuity and disaster recovery planning) rather than being altogether responsible for preventing the disruption from occurring.

8.7 As the cryptoasset sector expands and novel technologies are introduced, and as also outlined in SYSC 15A.4.3[R], we expect firms' mapping exercises to develop and evolve over time.

How our example firms may approach the mapping exercise

Firm A: Qualifying Stablecoin Issuer

Firm A maps the key components that support its important business service of stablecoin redemption. This includes on-chain smart contracts governing redemption mechanics, custodians holding reserve assets (an independent custodian to ensure the stablecoin is always fully backed and can be redeemed in a timely manner), external banking partners managing fund flows and off-chain monitoring systems ensuring compliance and liquidity.

The firm identifies critical third-party dependencies such as custodians holding backing assets, noting that any disruption in these areas could affect its redemptions. Firm A also maps relevant people and processes responsible for KYC checks, transaction validation and customer support.

Firm B: Qualifying Cryptoasset Trading Platform

Firm B maps the critical components supporting its important business service of order execution. This includes trading engine infrastructure, market data feeds, and order management systems. The firm identifies key third-party dependencies such as liquidity providers, external price oracles and custodial wallet providers enabling asset transfers. The firm gives particular attention to vulnerabilities like technology outages, smart contract failures or latency in execution that could disrupt order matching or price formation.

Firm C: Qualifying Cryptoasset Staking

Firm C maps the key components that support its important business service of validator node operation. This includes internal systems for staking management, custody of clients' cryptoassets and private keys, and interfaces with third-party validator infrastructure.

Firm C identifies its reliance on third-party technology providers as a key vulnerability, particularly the risk of downtime, performance degradation or misconfiguration leading to missed rewards or slashing.

Firm C: Qualifying Cryptoasset Staking

It also recognises that limited visibility into the validator's underlying infrastructure and controls can hinder timely response to incidents. This mapping supports Firm C's understanding of where operational risk lies across the service chain.

Firm D: Cryptoasset Custody

Firm D maps the full range of components involved in its cryptoasset custody service. This includes hot wallet infrastructure supporting real-time transactional access, cold storage vaults for secure asset safeguarding, key management systems, and third-party service providers such as HSM vendors. The firm highlights vulnerabilities such as reliance on permissionless DLTs and concentration risk among its custodial partners. Firm D's mapping also covers internal teams responsible for wallet access control and incident response.

Firm E: Intermediary Firm Arranging Deals

Firm E maps the key components that support its important business service of arranging orders for execution. This includes its internal systems for checking prices across multiple execution venues and for receiving and transmitting orders, which might be vulnerable to technology outages and server downtimes.

The firm also identifies critical third-party dependencies such as availability of execution venues to route orders to (such as trading platforms), external price oracles, and on/off ramp partners.

9 Conducting scenario planning and testing

9.1 As outlined in the previous mapping section, firms in scope of SYSC must first identify and map the resources that underpin their important business services. Building on this, SYSC 15A.5 requires firms to develop a scenario testing plan and carry out this testing to assess their ability to remain within the impact tolerances set for each important business service.

9.2 This section focuses on the requirements for both planning and executing scenario tests, incorporating considerations of the mapped resources and associated processes.

Scenario testing planning

9.3 In line with SYSC 15A.5.1[R], cryptoasset firms must develop a clear, detailed and regularly updated testing plan that sets out how they will gain assurance of their ability to remain within impact tolerances for each of their important business services. Given the rapid pace of innovation in the cryptoasset sector, regular updates to the testing plan are essential to maintaining effective operational resilience.

9.4 When developing this plan, firms should consider the non-exhaustive list of relevant factors set out in SYSC 15A.5.2[G]. Given the nature of cryptoasset business models,

firms should pay particular attention to designing testing scenarios that reflect their specific risks and operational dependencies, such as trading platform outages, redemption delays or failures in staking service delivery.

Scenario testing execution and documenting lessons learned

9.5 Complementing the scenario testing planning, firms must also execute scenario tests – as required under SYSC 15A.5.3[R] – to assess their operational resilience under severe but plausible disruption scenarios. Testing should include a diverse range of adverse circumstances varying in nature, severity and duration, relevant to cryptoasset business models.

9.6 Additionally, in line with SYSC 15A.5.6[G], firms should, among other things, aim to cover scenarios such as:

- Data corruption or loss (e.g. manipulation of wallet balances or transaction records).
- Critical third-party outages (e.g. custodian or blockchain node service disruptions).
- Failures in the technology (e.g. malicious node activity or oracle manipulation) and/or by people (e.g. insider threats) supporting their important business services.
- Compounded disruptions (e.g. simultaneous third-party outages and cyberattacks). To build resilience to cyberattacks, firms should maintain robust cyber controls and conduct penetration testing to monitor resilience of security and access systems.

9.7 When conducting scenario testing involving third parties, firms must ensure third-party testing methodologies are valid, effective and aligned with the firm's operational resilience requirements. Firms should also consider vulnerabilities to cyber risks arising from third-party dependencies. However, where testing directly with a third-party service provider (such as permissionless DLTs) is not possible, firms should use best alternatives where possible. As per SYSC 15A.5.5[G], firms remain responsible for following our testing requirements.

9.8 Following each test, and where actual operational disruption occurs, firms must conduct a lessons learned exercise in line with SYSC 15A.5.8[R] and maintain a written record of this in line with SYSC 15A.6.1[R]. This should identify any weaknesses exposed during testing or disruption and inform actions a firm must take to improve the firm's ability to effectively respond to and recover from future disruptions.

How our example firms might conduct scenario testing

Firm A: Qualifying Stablecoin Issuer
Firm A conducts regular reviews of resources that enable it to deliver its important business services as part of its annual business impact analysis. It designs severe but plausible scenarios, considering the potential impact of the redemption service and engages with the underlying DLT provider, including exploring ways to communicate with permissionless DLT communities where feasible. These tests indicate some residual risks and resilience gaps when faced with a severe but plausible scenario including those from DLT facing long-term disruption. Following a review of lessons learned, Firm A decides that it could use other DLTs

Firm A: Qualifying Stablecoin Issuer

as an additional service delivery channel to enable on-chain redemption. Among other actions, the firm also conducts a benchmarking exercise to identify alternate third-party firms that could enable redemption if the issuer has other technological issues.

Firm B: Qualifying Cryptoasset Trading Platform

Firm B carries out scenario tests that simulate failures in its order-matching engine and disruption of its post-trade data feed to the market. These tests cover severe but plausible scenarios, including sudden surges in trading volume, latency issues and outages at key third-party providers supporting the provision of post-trade transparency data.

The firm assesses its ability to maintain order integrity, switch to secondary trading infrastructure and preserve price accuracy for clients. Post-test analysis identifies a dependency on a single provider of post-trade data services as a resilience gap.

As a result, Firm B begins onboarding an additional provider.

Firm C: Qualifying Cryptoasset Staking

Firm C develops and maintains a scenario testing plan to assess its ability to remain within impact tolerance for its important business service of validator node operation. Scenarios include prolonged downtime or slashing events affecting its third-party technology providers.

As Firm C does not control validator infrastructure, its testing focuses on internal communications and controls. Simulated slashing scenarios are used to assess how effectively Firm C informs clients, manages internal escalation and maintains service transparency and identify any other risks it should mitigate.

Lessons learned exercises help improve client messaging, internal coordination and monitoring processes.

Firm D: Cryptoasset Custody

Firm D conducts scenario tests simulating a range of severe but plausible scenarios affecting its custody services. These include hot wallet compromises, cold storage access failures and internal access control breaches. These exercises validate Firm D's ability to isolate affected infrastructure, initiate backup procedures and restore access using secure off-site recovery systems. The tests also assess the resilience of its MPC protocols and coordination of its incident response and compliance teams.

As part of lessons learned, the firm identifies a gap in its visibility over outsourced key management hardware. In response, Firm D formalises assurance procedures with its third-party vendor and implements additional internal controls to independently verify the health and activity of its custody infrastructure.

Firm E: Intermediary Firm Arranging Deals

Firm E carries out scenario tests that simulate delays and disruptions to its order receipt and transmission and price checking systems. These tests cover prolonged server downtimes, significant pricing errors from external oracles, and access failures to on/off ramp partners. Firm E assesses the integrity of its backup

Firm E: Intermediary Firm Arranging Deals

servers, including during sudden surges in activity. Firm E also assesses the breadth of alternative execution venues to which it can route orders in case of disruption to a specific trading platform.

Post-test analysis identifies a dependency on a single large trading platform as a key execution venue. As a result, Firm E adds other execution venues to the options it uses to send orders for execution, reducing its reliance on any one venue. Following testing, Firm E also develops real-time data reporting tools to quickly identify outages or disruptions to the execution venues it sends orders to.

10 Communications

10.1 SYSC 15A.8 outlines effective communication strategies that are critical for cryptoasset firms to manage operational disruptions successfully and minimise harm to clients and other stakeholders. While these requirements and guidance are clear as currently set out, we have outlined examples below. These illustrate key scenarios where timely, transparent and technically informed external and internal communication, considered in advance of disruption, is essential to maintaining trust and ensuring clients are adequately supported.

10.2 Examples of disruptions requiring effective communication:

- **Disruptions outside the firm's control**: When operational disruptions arise from factors beyond the firm's direct control, such as a blockchain fork, clear and timely communication with clients is vital. Firms should promptly inform clients of the disruption, explain potential impacts on services or cryptoasset holdings, and provide guidance on any actions clients may need to take. They should provide regular updates throughout the event to ensure transparency and maintain client confidence.

Explanatory note – blockchain forks:

A fork occurs when a blockchain splits into two competing chains. The causes of forks can vary. In some cases, forks result unintentionally from the simultaneous creation of competing blocks, leading to a temporary divergence in the blockchain (hard forks). In other instances, forks are deliberate protocol upgrades that modify the rules governing the creation of new blocks (soft forks). For users of the blockchain, forks can lead to temporary disruptions, such as transaction delays or confusion over which chain to follow, and may sometimes require them to take action to ensure their assets remain secure and accessible.

- **Cyber security breach:** If a targeted hacking attack occurs, for example, unauthorised access to wallets, firms must promptly notify affected clients and stakeholders (e.g. through the firm's website and email notifications). Communications should include a clear summary of the incident, including the nature and scope of the breach, immediate containment actions (e.g. freezing transfers, isolating affected systems), and client-specific steps (e.g. resetting two-factor authentication, monitoring withdrawal history). Ongoing updates

should outline the status of forensic investigations, progress on asset recovery, and improvements to security controls.

10.3 In addition to the examples above, when assessing whether to report an operational incident based on reporting thresholds, firms should consider the non-exhaustive, high-level factors we set out in FG26/3 (paragraph 4.4).

10.4 In line with SYSC 15A.2.11[G], a firm should also notify the FCA of any failure to meet an impact tolerance.

10.5 This guidance aims to help cryptoasset firms develop and implement our operational resilience framework, helping them to maintain critical services, protect consumers and contribute to the stability of financial markets, even during periods of disruption. However, this guidance is not a complete description of the steps firms should take in ensuring operational resilience. Ultimately, it is up to firms to determine the extent of the analysis or review they need to confirm they meet our operational requirements in SYSC 15A.