



payments and crypto network

# FCA Cryptoasset authorisation: Operational Resilience for CASPs.

A quick-reference guide to FG26/6 — the FCA's finalised guidance on applying SYSC 15A operational resilience to cryptoasset firms.

# Operational failures in cryptoasset markets

FG26/6, published 30 June 2026, gives finalised guidance on applying the FCA's existing operational resilience framework (SYSC 15A) to cryptoasset firms. SYSC 15A is not new, having applied to FSMA authorised firms since 2022, however, the FCA is explicit that certain operational risks occur more often, or more severely, in cryptoasset markets than in traditional finance. These risks, as far as they apply to your CASP business model, will need to be reflected in your operational resilience framework. The guidance in FG 26/6 includes five fictional business models — a stablecoin issuer, a trading platform, a staking provider, a custodian, and an intermediary. If your firm operates a business model in one of these areas there is a worked example in the guidance that you can directly reference when developing your own framework.

## 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.

**Built on an existing framework:** FG 26/6 provides guidance specific to the cryptoasset industry as part of an existing operational resilience framework that has applied to FSMA-authorised firms since March 2022. See the FCA's 2021 Policy Statement PS 21/3 ("Building Operational Resilience"). These requirements include SYSC 4 (General Risk Management Requirements), SYSC 7 (Risk Control), SYSC 8 (Outsourcing) and SYSC 15A (Operational Resilience Requirements). These should all be reviewed as part of your work to develop an appropriate operational resilience framework for your business.

## The five illustrative business models in FG26/6

FG26/6 uses five fictional example firms to illustrate how the FCA's operational resilience requirements might apply in practice to the different example firms. While these examples are illustrative, the risks and scenarios described may be applicable to firms and should therefore be reviewed by all firms seeking to submit an application for authorisation as a CASP. Particular attention should be directed to examples that are relevant to your particular business model.

| FIRM          | BUSINESS MODEL                          | WHAT THEY DO                                                                                                                                                                                                                |
|---------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Firm A</b> | Qualifying stablecoin issuer            | Issues a fiat-referenced stablecoin across multiple permissionless DLTs, manages redemption and backing assets, and has embedded on-chain freeze functionality for stolen or illicit holdings.                              |
| <b>Firm B</b> | Qualifying cryptoasset trading platform | Provides retail and institutional clients with direct trading access via dedicated interfaces and APIs, running order-matching, liquidity pools and omnibus wallets. Outsources CDD identity verification to a third party. |
| <b>Firm C</b> | Qualifying cryptoasset staking          | Offers custodial staking across multiple proof-of-stake networks, delegating validator node operation to third-party operators under formal outsourcing arrangements while holding clients' private keys itself.            |
| <b>Firm D</b> | Cryptoasset custody                     | Safeguards cryptoassets across multiple blockchain networks using a hybrid cold/hot wallet architecture and multi-party computation (MPC) to split cryptographic keys, acting as clients' single point of access.           |
| <b>Firm E</b> | Intermediary arranging deals            | Routes client buy/sell orders to UK-authorised third-party execution venues in pursuit of best execution, and relies on a third-party on/off ramp partner for fiat and cryptoasset movement.                                |

## The FCA's framework and outsourcing expectations

Cryptoasset firms must apply the principles in SYSC 15A when identifying their Important Business Services, setting impact tolerances, mapping dependencies and conducting scenario testing. Under SYSC 15A.3.1R, firms must have sound, effective and comprehensive strategies, processes and systems in place and the FCA's guidance sets out three key focus areas that firms will need to factor into the development of their operational resilience framework.

- **Cyber and Technology Resilience** — firms should maintain robust and proportionate cyber and IT controls to ensure their systems supporting cryptoasset-related services are resilient, including managing risks to system availability, data integrity, third-party dependencies and recognised international cyber security standards and best practice.
- **Safeguarding Cryptographic Keys and Infrastructure** — where firms hold the means of access to a cryptoasset (e.g. private keys) or supporting infrastructure (e.g. smart contracts, validator nodes), they should establish secure, well-defined processes covering key loss, unauthorised access and general service disruption.
- **Continuity and Disruption Planning** — firms should create, test and regularly update plans to maintain or restore critical services during disruption, with scenarios reflecting their actual cryptoasset activities (e.g. smart contract failure, stablecoin reconciliation failure, validator outages), backed by targeted vulnerability scans, penetration testing, and evidenced monitoring and logging.

### FCA outsourcing expectations (SYSC 8)

Cryptoasset firms must also read this guidance with SYSC 8 in mind, applying appropriate skill, care and diligence to outsourcing arrangements in proportion to their nature, scale and complexity. Firms must notify the FCA when relying on a third party for operational functions that are critical or important to their services — in a cryptoasset context, this could include:

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

Permissionless DLTs are the exception, given that there is no direct contractual relationship with a service provider their use will not be treated as outsourcing (under SYSC 8.1.1R), however, firms are still expected to evaluate their internal operational controls for permissionless DLTs and remain fully responsible for their own operational resilience.

## Identify your Important Business Services

Everything else in an operational resilience framework flows from this first step: identifying the specific services which, if disrupted, would cause intolerable harm to clients or threaten the soundness, stability or resilience of the UK financial system or the orderly operation of financial markets.

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).

The FCA state that they are seeing cryptoasset services becoming more closely interconnected with traditional financial markets, increasing the potential for wider market contagion if disruptions occur. The FCA therefore encourage firms to 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].

### THE CORE TEST

#### What counts as an IBS?

A service provided by your firm — or by someone else on your behalf — where disruption could cause intolerable harm to clients, or threaten the soundness, stability or resilience of the UK financial system. Assessments must be kept up to date as your business changes.

### WORTH CHECKING FOR MULTI-ACTIVITY FIRMS

#### You likely have more than one

The FCA highlights that a firm combining activities — say, principal dealing alongside custody and staking — is likely to be underpinned by multiple important business services, not a single one. Each needs identifying separately.

### How each example firm identifies its IBS

- **Firm A** — the stablecoin issuer identifies redemption of its fiat-referenced stablecoin as an IBS. Holders rely on Firm A to convert stablecoins back into money; disruption could block access to redemption and undermine confidence more broadly, given the stablecoin's role in payments and trading.
- **Firm B** — the trading platform identifies matching and execution of orders as an IBS. A failure could disrupt market liquidity, impair price formation, cause client losses, and damage confidence in the platform and connected firms.
- **Firm C** — the staking provider identifies operation of validator nodes (run by third-party providers) as an IBS. If those providers fail, Firm C may be unable to distribute rewards and could face slashing penalties, causing financial loss to consumers.
- **Firm D** — the custody provider identifies providing and managing secure custody solutions as an IBS. Disruption could prevent clients accessing assets when needed, causing financial loss and greater exposure to market volatility, and may affect other firms relying on timely settlement.
- **Firm E** — the intermediary identifies receipt and transmission of orders for execution as an IBS. Disruption could impair market liquidity and execution quality, causing financial losses for clients.

## Setting impact tolerances

For each Important Business Service, firms must define the maximum level of disruption that is acceptable before harm becomes intolerable. Cryptoasset firms must be able to maintain their impact tolerance for each of their IBS if there is a severe but plausible operational disruption. Setting accurate impact tolerances ensures firms can effectively prevent, adapt, respond to and recover from operational disruptions.

| PRINCIPLE                    | WHAT IT MEANS IN PRACTICE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Per service</b>           | Each Important Business Service should be assigned its own impact tolerance — do not use a single firm-wide tolerance measure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Timeline</b>              | Establish a clear scale, measured by a length of time (and any other relevant metrics) that determines how long an Important Business Service can be disrupted before the firm exceeds its impact tolerance.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Calibrate tolerances</b>  | Calibrate tolerances to reflect the nature of the services, client base, and associated risks, considering the non-exhaustive list of relevant factors in SYSC 15A.2.7[G] and how demand for each Important Business Services may fluctuate, particularly during periods of heightened market activity.                                                                                                                                                                                                                                                                                                              |
| <b>Third-party alignment</b> | Where a third party delivers part of an IBS, firms must work with them to set impact tolerances and subsequently monitor the performance of the service provider against those tolerances on an ongoing basis. Examples of appropriately calibrating impact tolerances could 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. |
| <b>Multiple services</b>     | Since firms often operate multiple IBS there will likely be instances where firms suffers multiple disruptions within a short timeframe. While firms should consider the potential aggregate impact of disruption to multiple IBS when setting impact tolerances firms are expected to set their impact tolerances for each IBS with reference to a single disruption event rather than an aggregate of multiple disruptions. This approach is essential to ensure that impact tolerances remain a precise and reliable metric for the maximum level of disruption that can be tolerated.                            |
| <b>Active monitoring</b>     | Tolerances must be monitored continuously, with business continuity and contingency plans ready to trigger the moment a breach occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Map what each service actually depends on

Cryptoasset firms must identify and document the people, processes, technology, facilities and information needed to deliver each IBS in enough detail to support impact tolerance testing and help firms understand their vulnerabilities and remedy these as appropriate. For further information on the definitions of people, processes, technology, facilities and information you should refer to the FCA's Policy Statement 21/3 (Building operational resilience).

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.

Identifying risks and vulnerabilities as part of the mapping process will help to inform the development of testing scenarios. Some themes for vulnerabilities identified during mapping exercises are discussed in the guidance and are summarised below.

### Third-party arrangements

#### Vulnerabilities anywhere in the chain

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 their prescribed tolerance they should review, and where necessary, change their arrangements.

### Permissionless DLT

#### No counterparty means stronger internal controls

Where there is no direct contractual relationship, as with some permissionless DLTs, firms must strengthen internal controls and monitoring to identify and address vulnerabilities that traditional third-party oversight cannot reach. 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.

### Infrastructure beyond your control

#### Contingency, not control

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 FCA expect that the firm has appropriate remedies in place (e.g. business continuity and disaster recovery planning) in the event of a disruption rather than being responsible for preventing the disruption from occurring in the first place.

### Expected output

#### A mapped, mitigated picture

This stage should leave you with a defined set of people, processes, technology, facilities and information required to deliver each IBS (mapped to each IBS) and details of the vulnerabilities associated with these resource dependencies (either under your direct contractual control or arising from external network risk) and the mitigations that are in place.

## Scenario planning and testing

Following the identification and mapping of resources that underpin each IBS, firms must develop scenarios and perform testing to assess their ability to remain within the impact tolerances set for each IBS.

Firms will need to develop a clear and detailed testing plan, considering the list of non-exhaustive factors in SYSC 15A.5.2G and regularly review and update to keep pace with the innovation in the cryptoasset sector. Testing scenarios will need to be developed that reflect the firm's specific risks / vulnerabilities and operational dependencies (as identified during the mapping stage).

### DEVELOPING THE SCENARIOS

#### Scenario coverage

Scenarios should span a diverse range of adverse circumstances varying in nature, severity and duration — data corruption or loss, critical third-party outages, technology failures, and compounded disruptions all need consideration. The plan must be reviewed and updated regularly, and where testing involves third-party suppliers, firms should satisfy themselves the supplier's own testing methodology is valid and aligned with their requirements.

### AFTER THE TEST — OR A REAL INCIDENT

#### Lessons learned

Following each test, and following any actual operational disruption, firms must conduct a lessons-learned exercise in line with SYSC 15A.5.8R and keep a written record of it. This should identify any weaknesses exposed by the test or incident and inform actions a firm must take to improve its ability to respond to and recover from future disruption.

### Testing involving third parties

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.

# Communications

Effective communication strategies are critical for cryptoasset firms to manage operational disruptions successfully and minimise harm to clients and other stakeholders. 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.

The FCA provide two examples of disruptions requiring effective communication:

## Example 1

### 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.

## Example 2

### 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.

## Reporting to the FCA

- **Reporting operational incidents** — When assessing whether to report an operational incident based on reporting thresholds, firms should consider the non-exhaustive, high-level factors set out in the non-Handbook guidance FG26/3 (Operational Incident Reporting) published in March 2026.
- **Reporting a failure to meet impact tolerances** — in line with SYSC 15A.2.11[G], a firm should also notify the FCA of any failure to meet an impact tolerance.

# Building an authorisation-ready resilience framework

1

## Work through the four stages in order

Identify your Important Business Services (IBS), set impact tolerances, map dependencies (also identifying vulnerabilities), develop scenarios and then test your arrangements — each stage depends on the one before it.

2

## Read FG26/6 alongside PS21/3

FG26/6 illustrates how the existing operational resilience framework in SYSC 15A applies to cryptoasset business models — PS21/3 (Building operational resilience) remains the underlying source for how to build the framework itself.

3

## Run a test before you apply

Your application materials will need to describe your approach to operational resilience, and the FCA will expect you to answer detailed questions about it — a framework that has only ever existed on paper won't hold up under scrutiny.

4

## Prioritise the application window

If you are already providing cryptoasset services in the UK, submitting within the FCA's application window preserves your access to the saving provision (an important regulatory protection with commercial advantage) while the FCA assesses your application.

**Application window:** 30 September 2026 – 28 February 2027

**Regime commences:** 25 October 2027

Operational resilience is one of the areas the FCA has said it will probe most closely at authorisation.



## ABOUT PACNET

# A starting point for payments and cryptoasset firms

The Payments and Crypto Network (PACNET) is a compliance community for UK payment institutions, electronic money institutions and cryptoasset service providers. This guide is designed as a first point of reference: use it to orient yourself, then go to FG26/6 and PS21/3 themselves for the detail your operational resilience framework will need to rest on.

### Free guides and articles

Practical breakdowns of regulation and guidance for the CASP regime as it develops, written by compliance professionals for compliance teams. All materials available for download at our website: [www.pacnet.info](http://www.pacnet.info)

### Search and Quote tools

PACNET is developing tools for finding job opportunities (PACNET Search) and obtaining quotes from service providers (PACNET Quote).

### Slack community

400+ compliance professionals discussing compliance matters and opportunities. Sharing information and updates. Join for FREE via the link on our website: [www.pacnet.info](http://www.pacnet.info)

### The rest of this series

Previously published: The FCA CASP Authorisation Gateway, FCA Cryptoasset authorisation: Published materials, and FCA Cryptoasset authorisation: Application of the FCA Handbook.