

Operational Resilience for Cryptoasset firms

The FCA published operational resilience guidance for cryptoasset firms (FG 26/6) on 30 June 2026, building on a number of recent cryptoasset-focused Policy Statements ahead of the opening of the application window on 30 September 2026. Firms that are intending to submit an application for authorisation during this window should already be underway with their preparatory work, including building out their approach to operational resilience.

Why crypto firms should take Operational Resilience seriously

Operational resilience is not a new concept for existing FSMA-authorised firms that are subject to the requirements of the FCA's Handbook, including SYSC 15A on operational resilience. Payments firms, whilst not subject to many parts of the FCA Handbook, have also been required to implement an approach to operational resilience. For firms that are intending to be authorised by the FCA as a Crypto Asset Service Provider ("CASP"), the FCA's view that certain risks are specific, or likely to happen more often, in cryptoasset markets should be viewed as a sign that the FCA will pay particular attention to CASP operational resilience frameworks, either at authorisation or through supervisory attention (or both). For firms already subject to operational resilience requirements that are looking to become authorised as a CASP, the scope of risks contemplated will need to be expanded, for example, consideration of risks such as bugs in smart contract code, private key compromises, validator misconduct and slashing, and outages that lock clients out of their funds.

Another specific issue that increases the necessity for cryptoasset firms to maintain a robust operational resilience framework is that crypto markets run 24/7/365, compared to traditional financial services that have an opportunity to recover from disruption during quiet / closed periods. It also seems for crypto markets that the worst operational failures can coincide with the worst market conditions (volume spikes, volatility, panic affecting the market, systems and participants all at once). Size also matters here, the crypto market being relatively small and highly interconnected can suffer from system or sentiment driven panic that spreads very quickly and with often unanticipated impacts.

What does the FCA want to see?

FG26/6 does not introduce anything new, effectively sitting alongside the FCA's existing requirements as practical guidance for cryptoasset firms. It helpfully outlines five illustrative business models (issuer, trading platform, staking provider, custodian and intermediary) and provides some practical guidance for each. If your firm operates under one of these models you should certainly take a look at the relevant worked example to check your own thinking.

In terms of developing your specific approach, if you strip away the terminology, you should be asking four key questions in this order:

1. **What services, if they broke, would hurt someone?** Not "what do we do" in the purest sense. Specifically, which services would cause 'intolerable harm' to clients or threaten market stability if they failed. Firms with multiple business activities, for example, dealing, custody and staking services, usually find they have several of these "Important Business Services" per business activity. The guidance provides examples such as matching and execution of orders, operation of validator nodes, providing and managing secure custody solutions and receipt and transmission of orders for execution.
2. **How much disruption, for each service and incident, can we actually tolerate?** Clearly define impact tolerances for each Important Business Service (IBS) that represent the maximum level

of disruption to an IBS that its judged acceptable before further disruption causes intolerable harm. Firms must ensure they can maintain their impact tolerance for each of their IBS if there is a severe but plausible operational disruption. When setting impact tolerances firms should consider the non-exhaustive list of relevant factors in SYSC 15A.2.7[G].

3. **What do we depend on to deliver each of the identified services?** Identify the people, processes, technology, facilities, data, etc. upon which the IBS depend. Where firms have a DLT dependency, and no counter-party to hold accountable, the FCA acknowledge that this does not need to be treated as an outsourcing arrangement and the expectation shifts to stronger internal monitoring and contingency planning.
4. **Have we tested our arrangements?** Scenario testing against severe-but-plausible disruption must be performed, with lessons learned being documented and findings used to improve the framework. The feedback loop should support genuine operational advancement of the framework and not just be a documenting exercise (although this is important to evidence the work performed).

Permissionless DLT and outsourcing

The FCA have confirmed that using a permissionless DLT is not treated as an outsourcing arrangement under SYSC 8 since there is no direct contractual relationship with a service provider. Whilst not classified as outsourcing, the FCA expects firms using DLT technology to evaluate their internal controls around that dependency just as rigorously as they would with regard to outsourcing. The application of SYSC and other parts of the FCA's Handbook are covered in a previous article [here](#).

The importance of communication

The FCA's guidance is also clear with regard to the importance of a communication strategy as part of a sound operational resilience plan. The FCA provides example scenarios to illustrate 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.

If you do not, or are unable to, communicate clearly with clients and stakeholders in the event of disruption you are unlikely to achieve the objective of minimising harm as a result of a disruption. Also worth noting, if you breach an impact tolerance (set as part of your framework), you have an obligation under SYSC 15A.2.11G to notify the FCA.

What should firms be doing now?

Firms that are already FSMA authorised, or are authorised payments firms, will already be operating an operational resilience framework which will need to be updated, if an application for CASP authorisation is being sought, to account for crypto-specific activities. Review the crypto activities that will be provided to identify the component Important Business Services and associated resources required to deliver them.

For firms that are not already familiar with Operational Resilience requirements, the FCA's guidance FG 26/6 should be read alongside the requirements in SYSC 15A and PS 21/3 (Building operational resilience).

Either way, if you are preparing a CASP application for authorisation you will need to develop and describe your approach to meeting the operational resilience requirements (expecting that the FCA will scrutinise your framework in the context of the services provided and the business as a whole).