

Insights

THE ESSENTIAL GUIDE TO FCA CRYPTO AUTHORISATION - PREPARING A STRONG APPLICATION

Sep 30, 2026

Summary

The FCA's application window for the new UK cryptoasset regime opens on **30 September 2026** and closes on **28 February 2027**. Firms intending to carry on regulated cryptoasset activities when the regime commences on **25 October 2027** must now turn regulatory planning into an effective application strategy.

Applying for authorisation is not simply an exercise in completing forms and producing policies. Firms need to present a coherent account of their activities, business model, governance, financial resources, and systems and controls, supported by evidence that their arrangements will operate effectively in practice. The FCA is encouraging firms to submit timely, good-quality applications and to apply as soon as possible during the application period.

In this article, we summarise the key pillars of the new regulatory framework and identify five steps that can help firms prepare a strong application. The guide is relevant not only to crypto firms applying for authorisation, but also to other participants in the crypto distribution chain and mainstream financial services firms considering entering the market or assessing how the new regime may affect their existing activities and exposures.

The application window

The application window is now open. This is the point at which preparation becomes delivery.

Firms intending to carry on the new regulated cryptoasset activities will need either a new FCA authorisation or, if they are already authorised, a variation of permission. Existing registration under the Money Laundering Regulations (**MLRs**) does not automatically convert into FSMA authorisation. Nor does authorisation as a payment institution or e-money institution provide the necessary cryptoasset permissions.

Applying during the specified period is important to the availability of the relevant transitional arrangements. From 25 October 2027, firms carrying on regulated cryptoasset activities without the required authorisation, or the benefit of an applicable saving or transitional provision, risk breaching the general prohibition under FSMA.

In our Emerging Themes Technology series this year, we have examined the new regulatory perimeter for cryptoasset firms and the conduct, prudential and market-integrity requirements that will apply. This article brings that analysis together with a practical focus on preparing for authorisation.

Scope of regulated activities

The new regulated cryptoasset activities can be summarised as:

- Issuing qualifying stablecoins in the UK
- Safeguarding, and arranging safeguarding, of qualifying cryptoassets and relevant specified investment cryptoassets
- Operating a qualifying cryptoasset trading platform (**QCATP**)
- Dealing, and arranging deals in, qualifying cryptoassets as principal or agent
- Arranging qualifying cryptoasset staking

Firms should begin by classifying the relevant cryptoassets, mapping every function within their current and proposed operating models against the regulated activities framework and identifying the permissions that may be required. Our earlier analysis, [CP26/13: The FCA sharpens the cryptoasset regulatory perimeter](#), considers the perimeter in more detail.

Whether authorisation is required depends on what a firm actually does in substance and the role it performs. Labels such as “exchange”, “wallet”, “broker” or “platform” do not determine the regulatory outcome. A single business may carry on multiple regulated activities, each requiring its own permission. Arranging, safeguarding and staking activities may also capture functions embedded within a product flow that are not described in those terms externally.

For international firms, territorial scope requires particular attention. The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (the **Cryptoasset Regulations**) include provisions under which certain activities involving UK consumers may be treated as carried on in the UK even where the person carrying on the activity is established overseas. Critically, the overseas persons exclusion does not apply to the new regulated cryptoasset activities. International firms should therefore consider the UK nexus of their activities, alongside the allocation of activities between group entities and the identity of the appropriate applicant, as part of their permissions analysis.

Seven core pillars of the regulatory framework

The UK has brought cryptoasset regulation within the existing FSMA framework rather than creating a standalone regime. Authorised cryptoasset firms will therefore need to navigate regulatory frameworks familiar from traditional financial services, alongside requirements tailored to the characteristics of cryptoasset markets.

1. Market integrity: the Market Abuse Regime for Cryptoassets

The Market Abuse Regime for Cryptoassets (**MARC**) applies where a qualifying cryptoasset has been admitted, or is subject to an application for admission, to trading on a UK QCATP. The prohibitions on insider dealing, unlawful disclosure of inside information and market manipulation apply irrespective of where the relevant behaviour takes place. UK QCATPs and cryptoasset intermediaries must establish and maintain effective arrangements, systems and procedures to prevent, detect and disrupt actual or attempted market abuse. The regime also includes requirements relating to suspicious order or transaction notifications, insider lists and, for certain firms, cross-platform information sharing and on-chain monitoring.

2. Client asset safeguarding

Dedicated safeguarding rules apply to firms holding client cryptoassets, including through CASS 17. The FCA will expect firms to demonstrate that safeguarding arrangements work in practice, rather than relying on policies alone. Operating a QCATP and safeguarding assets held on it are distinct regulated activities, requiring separate permissions and controls. Sub-custody arrangements, third-party custodians and the operational steps that give a firm control over a client's assets all require careful mapping against the final rules.

3. Governance and individual accountability

The Senior Managers and Certification Regime (**SM&CR**) will require firms to identify relevant Senior Managers, allocate applicable prescribed responsibilities, and prepare Statements of Responsibilities. Governance arrangements must also enable firms to satisfy the FCA's Threshold Conditions. The assessment will go beyond documentation. Boards and senior management should understand how decisions are made in practice, who is accountable for key risks and how concerns are escalated.

4. Prudential resilience

The new capital and liquidity requirements are calibrated to cryptoasset business models. Firms will need to assess their actual and projected financial position against the final requirements and demonstrate that they have adequate resources to support the activities for which they seek permission. The final prudential package is more proportionate than the original proposals in some

respects, but application preparation will still require credible financial forecasts, stress testing and a clear assessment of the firm's capital and liquidity needs.

5. Consumer Duty

The Consumer Duty will apply across much of the new cryptoasset regime where retail customers are involved, although its application will depend on the activity and the firm's role in the distribution chain. Where the Duty applies, firms should consider product and service design, price and value, consumer understanding and consumer support alongside their proposed customer base and distribution model.

6. Financial crime

Financial crime obligations under the MLRs and FSMA will operate concurrently. Systems and controls developed principally for MLR registration may not be sufficient for FSMA authorisation and should be tested against the firm's wider business model, customer risks and proposed activities.

7. Financial promotions

The financial promotions and regulated activities perimeters remain distinct. A communication may be a financial promotion even where the underlying activity does not itself require FSMA permission. Websites, apps, social media, referral and influencer arrangements, and communications relating to token listings should therefore be reviewed alongside application preparation and as part of the firm's wider UK market strategy.

Navigating the FCA policy papers

Drawing on the FCA's summary of the principal materials for the new [cryptoasset regime](#), we have grouped the key documents below and added a 'Relevance' column to help firms navigate the framework and identify the materials most relevant to their activities.

Firm type	Principal materials	Relevance
All firms carrying on regulated cryptoasset activities	PS26/13: Applying the FCA Handbook and related guidance: ▪ FG26/5: Consumer Duty ▪ FG26/6: Operational Resilience ▪ FG26/7: international cryptoasset firms	Use these materials to benchmark the firm-wide framework: Handbook application, customer outcomes, governance, operational resilience,

	PS26/12: Prudential Requirements and related guidance consultations on: ▪ GC26/4: COREPRU ▪ GC26/5: CRYPTOPRU Final guidance awaited Aggregate Cost Benefit Analysis	international structure and financial resources.
Stablecoin issuers and firms safeguarding cryptoassets	PS26/10: Stablecoin issuance Bank of England/FCA approach to systemic stablecoin issuers Digital Securities Sandbox guidance (see Section 4)	Focus on backing assets, redemption, disclosures, safeguarding, custody chains and the interaction between FCA and Bank of England requirements.
Trading platforms, intermediaries, custodians, staking providers and firms involved in lending or borrowing	PS26/11: Regulated cryptoasset activities	Identify the activity-specific conduct and systems requirements arising from the firm's operating model, including execution, custody, lending, borrowing and staking.
Issuers, offerors, trading platforms and intermediaries involved in admission or trading	PS26/9: Admissions and Disclosures and Market Abuse Regime for Cryptoassets	Map responsibilities for admissions, disclosure, due diligence, inside information and market-abuse prevention, detection and reporting.
This is a practical navigation guide rather than an exhaustive list. The materials relevant to each firm will depend on its activities, business model, permissions and structure.		

Five steps to strengthen your application

1. Confirm the perimeter and permissions

Firms should classify the relevant cryptoassets, map each function within their current and proposed operating models against the new regulated activities and identify the permissions required. The FCA is encouraging prospective applicants to review the new activities and ensure that the permissions sought align with their business model and risk profile.

For more complex business models, the analysis should also consider how activities interact across the customer journey and between group entities, including the implications of territorial scope and the allocation of activities within international groups.

Getting this right at the outset matters because the permissions analysis informs the rest of the application. It determines which requirements apply, the information the FCA will require and whether the proposed applicant is the appropriate entity.

2. Test whether the business is operationally ready

The FCA expects firms to carry out a gap analysis against the FSMA requirements and identify where existing arrangements need strengthening. Firms should develop a realistic implementation plan, agreed at board level, which identifies accountability, required changes and how and when they will be delivered.

The key issue for applicants will be the extent to which they can evidence operational readiness across the areas relevant to their business, including governance, financial crime controls, prudential resources, safeguarding arrangements, market surveillance and operational resilience.

The gap analysis should distinguish between arrangements already operating effectively and those still requiring work. It should also identify the people, resources and costs required to close those gaps.

3. Build one coherent application

The application should tell a consistent story. The activities and permissions sought should align with the regulatory business plan, operating model, governance structure, financial forecasts and supporting policies. The FCA has published detailed information on the authorisation application form, setting out both the core information required from applicants generally and the crypto-specific information that will be required according to the firm's business model and regulated activities. Applicants remain responsible for the accuracy and completeness of the information supplied.

That calls for more than collecting documents from separate workstreams. Before submission, firms should assess the application for gaps and inconsistencies. The regulatory business plan should align with the permissions sought; the governance arrangements with how decisions will be

taken in practice; the financial forecasts with the proposed business; and supporting policies with the firm's actual activities and risks.

The objective is a clear, complete, and internally consistent account of the regulated business the firm proposes to operate.

4. Engage with the FCA deliberately

Pre-application engagement can be valuable, particularly where a proposed business raises complex or novel questions around the perimeter, permissions, operating model or structure.

The FCA's Pre-Application Support Service (PASS) is available to cryptoasset firms as part of the targeted support for firms preparing for authorisation. Engagement is likely to be most useful once the firm has undertaken enough analysis to identify the particular issues on which it needs regulatory input.

Focused engagement, supported by a clear description of the business and the issues on which regulatory input is sought, is likely to be more productive than approaching the FCA with questions that remain at an early stage of internal analysis.

The same discipline should continue after submission. Information supplied should remain accurate and consistent, and firms should be prepared to deal constructively and promptly with questions arising during the authorisation process.

5. Treat authorisation as a strategic decision

Authorisation should not be treated solely as a compliance project. The exercise may expose more fundamental questions about the appropriate applicant entity, group structure, product suite, customer base, geographic footprint and viability of particular activities under the new framework.

Some firms may conclude that changes to their operating model are appropriate before applying. Others may decide to narrow the permissions sought or reconsider activities that cannot be supported sustainably within the regulated business.

These are better treated as strategic decisions at the outset than discovered as inconsistencies during the authorisation process. A strong application should reflect not simply an understanding of the FCA's requirements but a deliberate and coherent view of the regulated business the firm actually intends to operate.

Looking ahead

The FCA is encouraging firms to apply as soon as possible during the application period to avoid disruption to their business. It also warns that poor-quality applications may be rejected where they do not contain the minimum information required.

Speed should not, however, come at the expense of quality.

The strongest applications will bring together accurate perimeter analysis, operational readiness and a coherent explanation of how the proposed business will meet the FCA's standards. The application should provide a clear, complete and internally consistent account of the regulated business the firm intends to operate.

To receive future updates and invitations to our crypto industry engagement events this autumn, please contact the authors to be added to our dedicated crypto distribution list.

Meet the team



Suhail Mayor

Associate, London

suhail.mayor@bclplaw.com

[+44 \(0\) 20 3400 4626](tel:+442034004626)



Samantha Paul

Counsel, London

samantha.paul@bclplaw.com

[+44 \(0\) 20 3400 3194](tel:+442034003194)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and

should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.