



payments and crypto network

FCA Cryptoasset authorisation: Application Requirements.

A quick-reference guide to what the FCA's cryptoasset application asks for — the core requirements every applicant completes and the business model-specific sections triggered by your specific permissions.

Two parts: what all applicants complete and what depends on your specific permissions

The FCA's "Information about the authorisation application form for cryptoasset firms" (published 8 July 2026) splits the application requirements into a Core set of requirements that every applicant must complete and a series of business model specific sections that depend on the particular permissions being applied for. From 30 September 2026, this will be the basis of the online application builder — the form is generated dynamically around the activities and permissions you select, so you should not see a section that does not apply to your business.

01

Core requirements

Four groups of questions that every applicant firm must complete, regardless of business model: Application details, Firm details and organisational structure, Business model and strategy, and Governance, compliance and risk.

02

Business model-specific

Six further sections — Stablecoin issuers, Safeguarding, Staking, Lending and borrowing, Intermediaries, and operating a Cryptoasset Trading Platform (CATP) — each triggered by the applicant's business model and associated permissions being applied for.

30 September 2026: the online application builder opens. Firms preparing now should have a clearly documented service description and be able to map their proposed services and functionality to the specific permissions that it intends to apply for. This will enable the dynamic application builder to produce the required sections for completion.

Why this matters for preparation: the activities that you select at the start (Dealing, Safeguarding, Stablecoins, Staking, Trading platforms) and the associated permissions and client types, determine everything that follows. Getting that selection right early avoids reworking policy documents and attestations later in the process. Without a clearly defined service description mapped to your required regulatory permissions the accuracy and efficiency of your application process, and ultimate chances of success, will certainly be at risk.

Application details

The starting point for every application: a set of questions about your firm and its intended business model. The answers here determine which sections of the application pack will be presented for completion, as described in the business model specific sections later in this guide.

1

Firm details

Country of incorporation and legal status.

2

Activities and Permissions

Selection of sector, activities (Dealing, Safeguarding, Stablecoins, Staking, Trading platforms) and the specific permissions attached to each activity you select.

3

Client types

Retail, Professional and/or Eligible Counterparty — this shapes certain requirements, including provision of information to clients and consumer protection obligations.

4

Supplementary questions

Further fine-tuning questions used to build the precise application package that you will be required to complete.

Build once, complete what applies. Because the form is generated from these answers, it's worth finalising your permissions strategy — including client type scope — before starting to draft supporting policy documents. A late change to permissions can add or remove entire business model-specific sections.

Firm details and organisational structure

This section establishes the identity and location of your firm, who runs it, who owns or influences it, and how it is structured day to day. Most of it will be familiar territory for firms already authorised or registered under other FSMA or MLR regimes.

Firm details

Firm name, financial year end, website, and address details (principal place of business, registered office, head office, invoicing address and any UK branch address), contact details for complaints, auditor contact, professional advisor and compliance roles.

Trading arrangements

Other regulators the applicant firm is authorised / regulated by, details of any in-progress applications (UK or otherwise), details of acquisitions, and network status.

Senior management functions

Form A application forms for each individual holding a Senior Management Function (SMF). These will need to be submitted as part of the application package together with supporting documents.

Controllers

Details of anyone — person or firm — with ownership or influence over your firm. Thresholds vary by firm type (Directive / Non-directive / Limited permission consumer credit). Each controller is entered by type — Individual, Corporate, Trust, Partnership — with identification and control details.

Close links

Details of any close links with other individuals or organisations.

Organisational structure chart

An upload showing how the firm actually operates — senior management, key decision-makers, reporting lines, responsibilities and headcount — together with parent companies, subsidiaries, group entities and ownership percentages. In practice this works best as two linked charts in one document: staff organisation and group structure.

Business model and strategy

Where you set out what the applicant business actually does, how it makes money, and how it is resourced. Do not underestimate the time that will be necessary to complete this section, in particular drafting the Regulatory Business Plan (RBP) and financial forecasts.

Permissions and limitations

The investment types applicable to each regulated activity you are applying for, together with any limitations and requirements attached to them. This is essentially a tick-box section.

Fees

Projected annual income, used to calculate applicable fees, including FCA fees and the FOS levy. Calculations should be aligned with your three-year financial forecast.

Financial forecasts

Historical financial statements (three years, if the applicant is already trading), a financial forecast with supporting notes and assumptions, and completion of the FCA's linked financial data template to capture baseline financial information (the version for payments and cryptoasset firms). The FCA provide a link to additional information on preparing your financial forecast.

Regulatory Business Plan (RBP)

A firm-tailored RBP covering the FCA's required information (an example is linked from the guidance), plus sector-specific detail for cryptoasset trading, dealing, and lending and borrowing activities. It would be advisable to draft a structure for your RBP, considering the FCA's example, the specifics of your firm and the objective to expedite the FCA's assessment of the application materials (the RBP typically sits as the centre of the application package).

Financial promotions

A set of questions triggered if your firm intends to approve financial promotions on behalf of unauthorised firms or individuals.

IT self-assessment and controls

You need to download and complete the FCA's IT self-assessment (link provided in the FCA guidance) to determine whether you also need to complete the Detailed IT Controls form. Both will need to be uploaded with your application.

Governance, compliance and risk

The final core section, and potentially the most document-heavy. Firms typically underestimate how long it will take to develop, document and implement appropriate regulatory compliance, inc. financial crime, policies and procedures; these typically take time to draft and operationalise to a standard that will meet FCA scrutiny during the assessment of the application.

Disclosure of significant events

Information on your firm's history, including any litigation, bankruptcy, administration, criminal proceedings, or licence refusals, revocations or withdrawals.

Financial crime prevention framework

Demonstrate how your firm meets legal and regulatory responsibilities for preventing financial crime (inc. complying with the Money Laundering Regulations). Upload risk assessments (Business Wide Risk Assessment and Customer Risk Assessment) and the underlying methodology used, policies (including suspicious activity reporting, sanctions, travel rule, transaction monitoring), operational procedures (including onboarding, screening, monitoring, escalation of alerts), and details of any outsourcing or third-party tools used (including supporting agreements).

Compliance Monitoring Plan (CMP)

Evidence that your firm understands the risks it faces and how it plans to control them in the form of a CMP. This should be tailored to your firm and its proposed activities, referencing relevant FCA rules and guidance that are applicable to the firm and the checks in place to ensure compliance, together with assigned responsibilities, check frequency and record-keeping arrangements. The CMP is a highly operational and should be used by your compliance team as the primary tool for coordinating and recording compliance monitoring activities.

Complaints policy

Submit your Complaints Policy document describing how your firm identifies and handles complaints in accordance with FCA timeframes, staff training arrangements, customer communication, dispute resolution and fair treatment and how complaints feedback is used to prevent recurrence of underlying issues.

Cryptoasset records management policy

How records of cryptoasset activity are created, stored, kept accurate and complete, and protected from loss, tampering or unauthorised access — including retention, retrieval and deletion, and the governance oversight (responsibility, monitoring, escalation) that sits over all of it.

Stablecoin issuers

Firms issuing qualifying stablecoins must complete this section.

- **About the firm's stablecoin(s)** — how your firm is involved in issuing qualifying stablecoins, the type (qualifying / non-qualifying), stablecoin details including name, fiat backing and the type of DLT used to issue it (private, public, permissioned, permissionless).
- **Redemption policy** — a policy document showing how redemption requests will be overseen and fulfilled, including guaranteeing fulfilment at full value within one business day, the redemption fee basis (amounts, calculations and how they are kept fair and reasonable to operating costs), handling redemption requests during periods of heightened stress, and the technology and infrastructure supporting the redemption process.
- **Stablecoin disclosures** — documents explaining how your firm will publish disclosures about its qualifying stablecoin(s), including the systems and processes used for disclosures (inc. how you produce and update published stablecoin disclosure), disclosures that you will publish on your website and in your Qualifying Stablecoin Cryptoasset Disclosure Document (QCDD), all meeting the requirements in CRYPTO 2.5.
- **Backing asset policy** — how backing assets are held and structured, including segregation, systems, controls and oversight to manage backing assets, maintain liquidity, resolve discrepancies, and confirm fiduciary duty.
- **Use of third parties — backing assets** — if relevant, provide details of any unconnected third parties involved in managing backing assets and why they were chosen. Information on the controls, monitoring, reporting and review arrangements and any SLAs, performance measures or governance processes should also be provided. A written acknowledgement of trust is also required to be uploaded.
- **Use of third parties — issuance** — provide details of any third parties used as part of stablecoin issuance, including third-party names, roles and obligations, contracts describing the agreed terms and provisions that allow information sharing, and due diligence performed on third-parties.
- **Expanded backing assets** — firms planning to use expanded backing assets must show how they meet the CASS 16 requirements, including uploading a document listing the backing assets that will be used, risk management tools, CASS 16 Annex 4 notification form, signed attestation, and custodian acknowledgement letter.

Safeguarding

For completion by firms applying to safeguard, or arrange for another firm to safeguard, cryptoassets. The FCA require applicants to provide details of its systems and procedures for maintaining accurate records of the cryptoassets held on behalf of each client.

- **Records and reconciliation policy** — provide the policy and procedures that show how your firm checks and maintains accurate books and records each business day, including the daily reconciliation methods, shortfall handling, governance and oversight (including who is responsible for reconciliations and how issues are escalated), plus a client-specific record template that will be kept for each client and which captures the type and quantity of cryptoassets held for the client, blockchain addresses for each cryptoasset, the nature of the client's claim, and who can affect a transfer.
- **Proof of safeguarding trust** — evidence of how your firm will act as trustee when safeguarding cryptoassets:
 - Trust operating approach — wallet types used, whether a trust is operated per client, client class, or virtual address, and the reasons for that choice given your business model.
 - Systems and controls — the systems, tools and processes that will be used to keep client cryptoassets separate from the firm's own assets, including the use of different virtual addresses to support segregation.
 - Draft trust agreement and disclosures — how client cryptoassets are held on trust, how ownership and segregation are recorded, and any draft client-facing disclosure documents.
- **Third-party custodian policy** — detail how third parties that are used to safeguard client cryptoassets are appointed and overseen, including written agreements and SLAs setting out how liability is assigned between the third party, the firm and the client, and evidence of due diligence and governance steps followed when making the third-party appointments.
- **Cryptoassets means of access policy** — security and organisational arrangements safeguarding access to client cryptoassets, including Means of access policy (showing the methods for managing and storing private keys), private key management and security mechanisms (including the technology and security controls used to manage and protect private keys), and a key-mapping record template linking private keys to client cryptoassets.

Staking, Lending and Borrowing

Two shorter business model-specific sections, both built around the same underlying theme of consumer understanding and protection. Firms will need to ensure that retail clients genuinely understand the risks of the services before they are exposed to them.

FOR STAKING PERMISSIONS

Staking

- **Staked qualifying cryptoassets** — specify the investment types offered for staking: qualifying stablecoins, or qualifying cryptoassets excluding stablecoins.
- **Consumer understanding** — explain how the firm will ensure that retail clients understand the risks associated with staking risk, including uploading a General information document (explaining the firm, the staking service and the risks (in line with CRYPTO 10.2), the Key terms of agreement (in line with CRYPTO 10.3), and a Client communication and consent policy which includes how retail clients will be given the general information and key terms of agreement, when express prior consent is required and how it is recorded, and how material changes to the general information or terms are notified to retail clients.

FOR LENDING / BORROWING PERMISSIONS

Lending and borrowing

- **Collateral management** — a signed attestation stating that the firm will have policies and procedures in place for borrowing limits and managing collateral throughout the loan term. The attestation must confirm the limits set for retail clients (e.g. loan to value ratios, margin calls or liquidation levels), the modelling and volatility used to set limits, prohibition on generating revenue from qualifying cryptoasset borrowing collateral, negative balance protection, safeguarding collateral, and consent for auto top-ups (see CRYPTO 9.7).
- **Consumer understanding** — policies, procedures and assessment ensuring retail clients understand the risks of lending and borrowing cryptoassets, including a key features document (providing firm details, a clear description of the service and the main risks that retail clients face when using the service), Key terms of agreement for the service, information explaining how the firm will provide retail clients with the key features document and the terms, how these documents will be updated to meet the requirements of CRYPTO 9.2, disclosure process, how express consent will be gathered, and a copy of the appropriateness assessment that will be used to check a retail client understands the risks (in line with COBS 10.2A).

Intermediaries

Firms acting as intermediaries must complete this section and attest that they have policies and procedures in place for dealing with qualifying cryptoassets for retail clients.

Admission to trading and execution venue policy

A signed attestation that the firm will have policies and procedures in place to only deal or arrange deals in qualifying cryptoassets for retail clients that meets the admission to trading requirements in CRYPTO 5.3, and for non-overseas retail and elective professional clients only execute orders on a UK qualifying execution venue in line with CRYPTO 5.2.

Dealing as principal

How conflicts of interest are managed when the firm trades on its own account while executing client orders, including Functional separation arrangements (explain any proprietary trading activities and their separation from client order execution, responsibilities, reporting lines and information barriers), and a signed Post-trade transparency attestation that policies and procedures are in place to publish post-trade transparency information (see CRYPTO 7.3).

Order handling and execution

How the firm promptly executes client orders, obtains the most favourable terms and oversees settlement, including Order execution policies and procedures (execution factors used, execution venues, price disclosure, where express consent is sought, commission and fees structure), Client order execution information that will be shared with clients and the format, and Client order handling policies and procedures (arrangements, systems and controls used to ensure the prompt execution of client orders, approach to aggregating and allocating client orders for own account).

Personal account dealing

Provide details of the policies and procedures preventing relevant persons from entering into personal transactions (see CRYPTO 5.8).

Operating a Cryptoasset Trading Platform (CATP)

Firms operating a cryptoasset trading platform (CATP) will need to complete this section. The requirements are significant, reflecting the scale and market risk involved in running a trading platform.

About UK branch

Rationale and considerations for applying via a UK branch of an overseas firm, including any reliance on an offshore liquidity pool.

Market making policy

Provide market making policy documents used to identify customers who act as market makers on your cryptoasset trading platform and how their activity will be monitored. The information will need to explain whether your firm will enter into any legal, contractual or incentive arrangements and how these arrangements will be disclosed to customers and an explanation of the arrangements that have been designed to support fair, orderly and efficient trading and how compliance with platform terms will be monitored.

Algorithmic trading policy

Policies that explain the rules that will apply to algorithmic trading on the platform (see CRYPTO 6.4.2 and 6.4.3), including disclosure of information about algorithmic trading that are fair, clear and not misleading (see CRYPTO 6.4.5(2)). An example of the algorithmic trading disclosure (template or example) will need to be submitted.

Platform access policy

Policies explaining how the cryptoasset trading platform operates for clients, showing how you give users fair and orderly trading and restrict retail trading to qualifying cryptoassets. Operating rules (including access rules / criteria, ensuring execution efficiency, cryptoasset admission / withdrawal criteria, retail protections including QCDD signposting and overseas asset restrictions), Technical operations procedures explaining the arrangements used to manage technical operations and how these operating rules are published (i.e. a template showing the information that will be published in a way that is fair, clear and not misleading).

Conflicts of interest policy

Policies and procedures must be in place to identify and manage conflicts of interest relevant to the cryptoasset trading platform, including issuance-related conflicts (CRYPTO 6.2.4), personal account dealing by employees or connected individuals (CRYPTO 5.8), and in relation to settlement oversight and risk mitigation.

Trading framework

How the firm runs the platform and manages operational risk to meet the requirements of CRYPTO 6 and 7, including risk identification, management and mitigation, ensuring that trading systems are effective and appropriate for the nature and scale of the business (see CRYPTO 6.3.2), controls preventing disorderly markets (CRYPTO 6.3.7), and resources and backup facilities supporting pre- and post-trade transparency (CRYPTO 7).

Admission, market abuse and transparency

The second part of the CATP requirements, focus on the rules governing what cryptoassets are admitted to the trading platform, how market abuse is detected and prevented, publishing post-trade information and, if relevant, how the firm manages its own trading activity alongside the platform that it operates.

- **Admissions to trading criteria** — a rulebook explaining how the platform admits qualifying cryptoassets and qualifying stablecoins for trading on the platform, including Admission criteria policies and procedures (risk based objective criteria to assess admission, how the factors listed in CRYPTO 3.2.2 are considered, review and approval process, publishing the criteria on the website, and managing conflicts of interest) and a Rulebook and related procedure documents (setting out the provision of disclosure documents QCDDs, admission, form and content in accordance with CRYPTO 3.4 and withdrawal rights).
- **Market abuse detection and prevention** — a framework of policies, procedures and systems to detect and prevent market abuse on the platform (CRYPTO 4.7):
 - Detection policies covering transaction monitoring, activity in cryptoassets being admitted to trading, and the halting, suspension or restriction of trading.
 - Systems and controls for responding to suspected market abuse, including receiving and assessing notifications of suspicious orders from intermediaries and halting, suspending or restricting activities when needed.
 - Platform-specific rules and procedures for preventing and disrupting market abuse on the cryptoasset trading platform, including the tools and controls used to disrupt market abuse, information barriers, and personal account dealing rules.
- **Post-trade transparency** — how post-trade information is published after a qualifying cryptoasset transaction executes on the platform (see CRYPTO 7.3.4), including Post-trade transparency policies and procedures (detailing how qualifying transactions will be identified and post-trade information publishing process) and the platform's Deferral policy (including criteria used to decide whether a transaction benefits from a post-trade transparency deferral and how such criteria will be applied consistently).
- **Trading on own account** — where the firm trades on its own account while operating a cryptoasset trading platform it must have policies and processes in place to ensure that its own account trading takes place outside of its platform, including details on the systems and controls that stop the principal trading desk accessing the CATP to execute trades, customer disclosure to make clear they are dealing with the principal trading desk not the CATP, and the identification and management of conflicts of interest.
- **Matched principal trading policy** — for firms trading on a matched principal basis on their platform there must be policies and procedures in place to manage and oversee this trading, including Governance and oversight process (responsibility for oversight, governance arrangements and escalation procedures), Systems and controls (including technology that supports matched pricing, risk management processes, checks and limits) and how settlement risk is minimised.

Large CATPs (>£10m projected revenue over 3 years)

Firms projecting more than £10 million in revenue over three years must additionally demonstrate how they will meet enhanced transparency duties and detect and report suspected market abuse on their platform.

A starting point — not a substitute for the source document

This guide summarises the FCA's "Information about the authorisation application form for cryptoasset firms" (published 8 July 2026) to help prospective CASP applicants understand the core and permission-specific submission requirements. This guide sits alongside the rest of PACNET's guides on CASP authorisation (all available from www.pacnet.info and our free to join Slack channel) and should be read together with the FCA's own published guidance.

Map your permissions first

Confirm your activities and client types early (i.e. agree and document a service description and map it to the regulatory permissions) since this will help you determine which business model-specific sections of the application will apply to your firm. Without this clarity your application is significantly at risk.

Start policy drafting early

Drafting the numerous policy and procedure documents will take time. Some documents will take significant time. It is critical that there is consistency across documentation leading into the application materials themselves. Early drafting will help you achieve the necessary level of detail and consistency. The FCA's "ready, willing and organised" authorisation threshold requires applicant firms to have operationalised their procedures (to the extent possible) and for this to be demonstrated during the assessment of the application. Early drafting of policies and procedures is the only way to achieve this requirement.

Use the primary sources

This guide is deliberately high-level. Refer back to the FCA's application form guidance and the relevant CRYPTO, CASS, COBS and SYSC sourcebook provisions before finalising any submission.

Get in touch

If you are preparing a CASP application and want help working through the core or business model specific requirements, feel free to get in touch!



payments and crypto network

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 the FCA's own application form guidance for the detail your submission 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

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

The rest of this series

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

For informational purposes only — not legal advice. Always refer to FCA published materials for current requirements.
fca.org.uk · www.pacnet.info · © 2026 Payments and Crypto Network Limited.