HACKEN

UK Crypto FCA Authorisation: Cybersecurity & Operational Resilience Checklist

A practical checklist for firms preparing for the UK's cryptoasset authorisation regime. Use this checklist to identify gaps and organise the evidence supporting your application.

01 — Governance and accountability

- [ ] A named senior owner is accountable for cybersecurity and operational resilience
- [ ] The board approves and reviews cyber risk appetite and receives decision-useful security reporting
- [ ] Security responsibilities, escalation routes and relevant SM&CR responsibilities are clearly allocated
- [ ] Material cyber decisions, risk acceptances and exceptions are documented

02 — Important business services and operational resilience

- [ ] Important business services and their impact tolerances are defined
- [ ] People, technology, data and third-party dependencies are mapped to each service
- [ ] Scenario testing demonstrates the firm's ability to remain within impact tolerances
- [ ] Testing covers relevant crypto-specific scenarios, such as validator or chain failure, smart-contract failure, reconciliation failure, cloud outage, bridge failure, chain reorganisation or oracle manipulation

03 — Private keys and wallet infrastructure

- [ ] Key-generation and the full key lifecycle are documented and controlled, including storage, signing, rotation, backup, recovery and destruction
- [ ] Segregation of duties prevents unauthorised individuals from independently moving client assets
- [ ] Hot, warm and cold wallet arrangements have documented security rationales
- [ ] MPC, multisig and HSM controls are threat-modelled and appropriately governed
- [ ] Seeds, shards, recovery keys and administrative keys are inventoried and protected
- [ ] Signing activity is logged and reviewable
- [ ] Key-loss, unauthorised-signing, backup and recovery procedures have been technically tested

04 — Smart contracts and protocol security

Complete this section where smart contracts are material to the firm's regulated activities.

- [ ] Smart contracts follow secure development and controlled change processes
- [ ] Independent security reviews are completed before material releases
- [ ] Oracle, validator and other protocol dependencies are documented and mitigated
- [ ] Upgrade keys, proxy contracts and emergency controls have named owners and controlled access
- [ ] On-chain monitoring can detect abnormal behaviour
- [ ] Response procedures cover relevant exploits, bridge failures, chain reorganisations and contract freezes

05 — Security testing, detection and incident response

- [ ] Vulnerability scanning and penetration testing cover relevant infrastructure, applications, APIs, cloud environments, endpoints, customer journeys and privileged functions
- [ ] Wallet and transaction-signing infrastructure receives specialist testing where relevant
- [ ] Logs support investigation and can be produced as regulatory evidence
- [ ] Incident classification, notification and escalation procedures account for applicable FCA requirements
- [ ] Tabletop exercises involve relevant senior management, legal, compliance and communications stakeholders
- [ ] Incident-response and recovery procedures are maintained, tested and updated
- [ ] Findings, remediation and lessons learned are tracked to closure

*This checklist is a practical readiness aid, not legal advice. Applicable FCA requirements depend on the firm's activities, permissions, structure and circumstances.

06 — Evidence and application readiness

- [ ] Security architecture, asset inventories, dependency maps and key-management procedures reflect the current operating environment
- [ ] Penetration tests, smart-contract reviews and scenario exercises have documented results and remediation evidence where applicable
- [ ] Security metrics, board reporting and the cyber risk register demonstrate control performance, weaknesses, owners and treatment decisions
- [ ] Wallet-control matrices document who can move assets and which approvals are required
- [ ] Third-party assessments and due-diligence records are retained
- [ ] Every material security claim in the FCA application can be traced to supporting evidence
- [ ] Material findings have owners, remediation plans and deadlines, with evidence available before submission

07 — Third parties and critical dependencies

- [ ] Material third parties and dependencies are inventoried and mapped to important business services
- [ ] Due diligence covers security, resilience, concentration and exit risk
- [ ] Contracts provide appropriate audit, incident-notification, access and termination rights
- [ ] The firm can continue or recover critical operations if a major provider fails
- [ ] Outsourcing arrangements are assessed against applicable FCA requirements
- [ ] Management understands that outsourcing does not transfer regulatory responsibility

Found compliance gaps?

Define your readiness for FCA authorisation with a compliance expert.

Book a 30-min call →

*This checklist is a practical readiness aid, not legal advice. Applicable FCA requirements depend on the firm's activities, permissions, structure and circumstances.