payments and crypto network

FCA Cryptoasset authorisation: Financial Crime Risk Assessments for CASPs.

A practical guide to establishing a financial crime risk assessment methodology and using it to assess the risks faced by a cryptoasset business.

www.pacnet.info

BEFORE YOU START ASSESSING

Financial crime risk assessment methodology

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (“MLR”) require firms to operate a risk-based approach towards the prevention of financial crime, starting with an assessment of the financial crime risks that are relevant to the business and its services. A methodology based on the standard risk areas: customer types, products, transactions, delivery channels and countries of operation should be developed by CASP applicants. This guide sets out, practically, how to agree a suitable methodology and then use it to perform (and keep current) your financial crime risk assessment.

01

Agree the methodology

Before assessing anything, agree how financial crime risks will be identified, categorised and scored. The process for financial crime risks should align, and form part of, the overall enterprise-wide risk assessment framework. Risk Categories for ML / TF / PEP / Sanctions risks will need to be developed. Impact and Likelihood scoring would align with the broader risk management framework. A financial crime Risk Appetite will need to be set (and agreed by the Board).

02

Perform the assessment

Apply the agreed methodology to the firm's actual business: identify the specific risks and any associated mitigating controls, record both in the Risk Register, score the risks before the application of mitigating controls (Inherent Risk) and after (Residual Risk), and compare the result against Risk Appetite (for financial crime).

03

A living document

The risk assessment is not a one-off exercise for authorisation. It will need to be maintained by the MLRO on an ongoing basis, including review of risks, mitigating controls and the Inherent and Residual Risk assessments at a frequency that is determined by the severity of each risk. Risks and controls will need to be updated as the business, typologies and regulatory landscape evolve. New risks should be added and, where appropriate, old risks removed.

Why this matters: the MLR requires firms to "take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject" and to keep an up-to-date written record of the steps taken. The financial crime risk assessment also underpins the development of the AML/CTF policies, procedures and controls that will need to be described in the application and submitted by way of supporting documents.

METHODOLOGY OVERVIEW

Components of your risk assessment methodology

A complete financial crime risk assessment methodology brings together various components — an overview of the key parts is provided below.

Risk categorisation

Risk Categories (e.g. customers, products and services, transactions, delivery channels and countries of operation) with cryptoasset-specific sub-categories, will need to be developed to facilitate the organisation of how risks are documented and reported.

Ownership

Responsibility for the operation / update of the methodology should be clearly assigned. Whilst the financial crime risk assessment would likely be a responsibility of the MLRO, the methodology itself should be applied on an enterprise-wide basis and may be the responsibility of a Risk Manager / CRO. The methodology should be approved by the Board.

Risks and mitigating controls

The identification of risks and associated mitigating controls is central to the operation of the risk management framework. The methodology should consider how this is done (inc. implementing risk management across three lines of defence), using Risk Factors (described later) and typologies. Identified risks and mitigating controls should then be documented in your Risk Register.

Risk assessments

Each risk needs to be scored in order to prioritise them for treatment. The methodology needs to define how risk is assessed on an agreed scale, in terms of Impact and Likelihood. Scoring before mitigating controls are applied (Inherent Risk) and after (Residual Risk) and a review frequency (linked to Inherent severity) should also be included in the methodology.

Risk appetite

Risk appetite is the level of risk that is acceptable in order to achieve the strategic goals defined by the Board. Risk appetite will differ between risk categories. In the context of financial crime, the level of risk that the firm is willing to accept should be low. Risk appetite should be set by the Board, typically by Risk Category. Residual Risk (after applying the mitigating controls) should be below Risk Appetite for that category. If not, you need to either strengthen the mitigating controls or reduce / avoid the Inherent Risk.

Combining risk scores

How individual risk scores are combined (typically averaged) into an overall rating for each Risk Category, and across categories into the firm's overall financial crime risk profile.

Risk reporting

Regular management information should be provided to the Board to facilitate their oversight responsibility. Management information from across the business should be provided in a Board Reporting Pack distributed to all directors ahead of each Board meeting. This regular reporting cycle helps evidence the operation of the business, Board oversight and decision-making. In the context of financial crime, there should be a separate section in the pack to cover updates in regulation, policies, operation of procedures, metrics such as internal and external suspicious activity reports, etc. The reporting of an Annual MLRO Report, summarising developments in, and operation of, the financial crime framework is also important. Board approval of financial crime policies and updated risk assessments is key to oversight and control requirements and also involves reporting updates, reasoning and approval requirements.

METHODOLOGY — 1 OF 3

Developing your risk categories

Risk Categories will need to be developed to help you classify and organise the financial crime risks that you have identified. Developing a suitable set of Risk Categories will help the setting of risk appetite, mitigation, assessment and reporting of risks. The Joint Money Laundering Steering Group ("JMLSG") and the MLR both point to the same high-level categories, which are listed below. These would logically be used as the top-level Risk Categories with sub-categories developed to provide any necessary granularity. Applicant CASP firms should start with these top-level categories and develop sub-categories that reflect cryptoasset-specific risks. Risk Factors are also detailed below for various risk areas / categories to help firms identify and develop the risks that will be documented in the Risk Register.

- **Customers and beneficial owners** — retail vs institutional clients, use of corporate or trust structures, politically exposed persons, customers transacting with self-hosted (unhosted) wallets, and customers whose source of funds or wealth originates from cryptoassets rather than traditional finance.
- **Products and services** — custody and safeguarding, staking, exchange and trading (as principal or agent), stablecoin issuance, and any product feature that allows rapid conversion between cryptoassets and fiat.
- **Transactions** — transaction size, volume and velocity, peer-to-peer transfers, large or structured deposits/ withdrawals, and transactions involving privacy-enhancing tools such as mixers, tumblers or privacy coins.
- **Delivery channels** — non-face-to-face onboarding, API-based or white-label access, and reliance on third parties such as introducers, agents or other VASPs in the transaction chain.
- **Countries of operation** — jurisdictions with weak or no VASP (Virtual Asset Service Provider) registration regimes, sanctioned or high-risk jurisdictions, and counterparty exposure to exchanges or wallets domiciled in such jurisdictions.

> **Risk Factors help to drive granularity:** each Risk Category should be broken down into sub-categories to add the necessary granularity to your risk categorisation. The Risk Factors listed above will help identify suitable sub-categories for your CASP firm and the identification of individual risks. The right breakdown ultimately depends on the firm's own products, customers and scale.

Scoring Inherent and Residual Risk

Once a risk has been identified, categorised and recorded in your Risk Register, it will need to be scored / assessed twice: once before the mitigating controls are applied (Inherent Risk) and once after (Residual Risk). The same scoring methodology should be used for both Impact and Likelihood and be aligned with the scoring used in the firm's enterprise-wide risk framework. This will ensure that financial crime risks sit comfortably alongside other risks and can therefore be reported on a comparable basis.

Inherent Risk

The risk in its unmitigated state — before any mitigating controls are applied. Scored using Impact and Likelihood (according to the agreed methodology, e.g. each on a five-point scale) and combined to produce an overall rating, e.g. Low, Medium, High or Extreme.

Mitigating controls

The specific controls that reduce the risk — for example, enhanced due diligence for self-hosted wallet counterparties, blockchain analytics screening, or transaction monitoring rules tuned to cryptoasset typologies.

Residual Risk

The risk that remains after the mitigating controls are applied, scored using the same Impact / Likelihood scale. This is the assessment that is compared to the Risk Appetite (for that Risk Category). If the Residual Risk sits above the risk appetite, your mitigating controls need strengthening.

Risk Appetite

The level of risk the firm is willing to accept, set separately for Inherent and Residual Risk, by Risk Category and on an overall basis. Residual Risk Appetite for financial crime is typically set at Low.

Example scoring matrix: Impact and Likelihood are each scored 1 to 5 (for example, Likelihood from "Unlikely" to "Almost certain" and Impact from "Insignificant" to "Catastrophic"), and the combination of the two scores is read off a matrix to give an overall rating of Low, Medium, High or Extreme. Using the same matrix as the firm's wider enterprise risk framework keeps financial crime risk comparable with other risk types reported to the Board.

Risk appetite, review frequency and reporting

With risks identified, categorised, recorded in your Risk Register together with the associated mitigating controls, and scored, the methodology will need to define how often each risk will be reviewed, how individual scores are combined for reporting, and how risk management information is provided to the Board.

Risk Appetite

Risk appetite is the level of risk that a business is willing to accept in pursuit of a desired reward, e.g. achieving its strategic goals. It is a measure of how much uncertainty a business would tolerate in pursuit of a particular goal. Risk appetites can vary greatly between different businesses, as well as between the different risk areas within a specific business.

A ‘high’ risk appetite would indicate that the management of a business are willing to take on significant levels of risk in order to achieve their objectives. This could be a willingness to take on risk across the business as a whole or within certain areas of the business. A high risk appetite should not apply to financial crime risk which would typically be set to low. The risk appetite of the business should be set by the Board.

Combining scores

Individual risk scores within each Risk Category should be combined (typically averaged) to give an overall rating for that specific category. The methodology should also define how scores can be combined across Risk Categories to provide the firm's overall financial crime risk profile.

Review frequency

Documented risks, mitigating controls and assessments of Inherent Risk and Residual Risk should be reviewed on an ongoing basis. The frequency could be based on the severity of the Inherent Risk (which is the most logical approach since it forces a review of the risk and control based on the raw state of the risk), e.g. a risk with an inherent score of Extreme or High warrants frequent review even where controls currently bring it down to a Low residual rating, since it is the continued effectiveness of those controls that is also being tested.

Reporting to the Board

Risk management information should be reported to the Board on a regular basis. A ‘Board Reporting Pack’ could be used to provide management information to the Board ahead of each meeting and include a distinct section for financial crime. An Annual MLRO Report should be provided by the firm's MLRO and formal Board approval of financial crime policies and updated risk assessments sought.

Record keeping

Records should be kept in accordance with the firm's agreed record keeping policy (duration, location, format). The documented risk methodology, Risk Register, prior versions of each financial crime risk assessment, financial crime typologies, reported management information should all be retained. Appropriate record keeping is not just good governance, it is a regulatory requirement of the MLR and an expectation of the FCA.

Inherent Risk rating	Indicative review frequency
Extreme	Quarterly
High	Half-yearly
Medium	Annual
Low	Every two years

Ad-hoc reviews sit alongside this regular cycle — triggered by a new product, customer segment or geography, a new outsourced provider relevant to financial crime controls, or a material change in the external risk environment.

FINANCIAL CRIME TYPOLOGIES

Cryptoasset financial crime typologies

Typologies are scenarios describing how a business or its services could be used for financial crime and are maintained by firms as the basis for identifying financial crime related risks. CASP firms should maintain a documented set of typologies that reflect cryptoasset-specific vulnerabilities. These will differ from the typologies that payments firms maintain, although there may be some similarities. The typologies maintained by a CASP should include, where relevant, those published by the cryptoasset industry. Some examples of the types of typology areas are provided below as a starting point and could be used to develop detailed typologies with input from product, customer-facing and fraud expertise.

- **Mixing services and privacy coins** — use of mixers, tumblers or privacy-enhancing cryptoassets to break the audit trail between source and destination of funds.
- **Self-hosted wallet counterparties** — transfers to or from wallets not held by a regulated custodian, where beneficial ownership and source of funds cannot be independently verified.
- **Cross-chain bridges and chain-hopping** — rapid movement of value across multiple blockchains or asset types to obscure the transaction trail.
- **Structured deposits and withdrawals** — multiple transactions kept below reporting or monitoring thresholds to avoid detection.
- **DeFi protocol interaction** — use of decentralised exchanges, lending protocols or liquidity pools to layer funds without a regulated intermediary.
- **High-risk jurisdiction exposure** — counterparties, IP addresses or wallet clusters associated with jurisdictions lacking VASP regulation, or subject to sanctions.
- **OTC desk and large-value trade risk** — bilateral, off-platform trades that bypass standard onboarding or monitoring controls.

> **Keep typologies current:** the financial crime typologies documented by your firm should be reviewed on an ongoing basis, certainly at least annually, to ensure that they remain up to date in light of the development of your firm, the services provided and changes within the cryptoasset industry / market. The review would typically be led by the MLRO since the typologies are critical for the development of the risk-based financial crime controls.

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 MLR, JMLSG guidance and the FCA's Financial Crime Guide for the detail your methodology 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, FCA Cryptoasset authorisation: Operational Resilience for CASPs, FCA Cryptoasset authorisation: Application Requirements, FCA Cryptoasset authorisation: Preparing your Regulatory Business Plan, and FCA Cryptoasset authorisation: Financial Forecast and Capital Requirements.

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.