Guidance consultation

Non-Handbook Guidance on CRYPTOPRU 7: Overall risk assessment for CRYPTOPRU firms
GC26/5

June 2026

1 Introduction

Why we are consulting

1.1 We are developing non-Handbook guidance (NHG) to accompany the relevant sections on the overall risk assessment (Chapter 7) in the new prudential sourcebook, CRYPTOPRU. The guidance sets out our expectations around the purpose and scope of the overall risk assessment for CRYPTOPRU firms. It forms a part of our wider strategy to enhance the accessibility of our rules by distinguishing supporting material from core Handbook content. We expect this to make it easier for firms to navigate the requirements and support consistent adoption of the prudential standards.

1.2 In CP 25/15: A prudential regime for cryptoasset firms[1], we proposed an integrated prudential sourcebook (COREPRU) covering the core prudential requirements common across different types of firms we prudentially regulate. Where necessary, COREPRU is supplemented with sector-specific prudential sourcebooks, such as CRYPTOPRU.

1.3 In December 2025, we published CP 25/42: A prudential regime for cryptoasset firms[2], which sets out our proposals on the overall risk assessment in both COREPRU and CRYPTOPRU. This is a continuous assessment process undertaken by firms to ensure they have adequate financial resources.

1.4 We have now published the final rules consulted in the above CPs as part of PS26/12: A prudential regime for cryptoasset firms. This NHG sets out our expectations in

[1] CP 25/15: A prudential regime for cryptoasset firms

[2] CP 25/42: A prudential regime for cryptoasset firms

relation to our rules in PS 26/12. It is tailored for use by firms' management teams and focuses on the purpose of the overall risk assessment rather than detailed steps needed to comply with the rules. We aim to provide clarity on our expectations, supporting predictable and proportionate regulation. Our purpose is to help firms hold adequate resources at all times, supporting their ability to operate effectively and compete internationally.

1.5 Firms should also refer to the proposed NHG for COREPRU 7, which is relevant to CRYPTOPRU firms, and is likewise undergoing a consultation process.

Who this applies to

1.6 This guidance consultation covers firms seeking authorisation and regulation for the Regulated Activities outlined in the Cryptoassets Regulations.

1.7 Who else needs to read this document:

- Firms that participate in, or support the services of, regulated cryptoasset activities.
- Industry groups, law firms and trade bodies representing firms in the cryptoasset sector.
- Professional advisers in the cryptoasset sector and law firms.
- Consumers and groups representing consumer interests.

1.8 It may also interest:

- Policy makers and other regulatory bodies.
- Academics and think tanks.
- Industry experts and commentators

Outcomes we are seeking

1.9 This consultation seeks feedback on proposals for guidance on how firms complete the overall risk assessment to comply with the CRYPTOPRU regime. Annex 1 contains the draft guidance on which we are consulting.

1.10 We received considerable feedback from industry asking for more guidance on implementing our rules. We have also observed from several multi-firm reviews, variation across firms in their approaches to assessing risk and adequate financial resources.

1.11 We expect this guidance will support CRYPTOPRU firms in developing more mature risk management practices. Many of these firms are less familiar with prudential frameworks, having not previously operated within such regulatory regimes.

1.12 This guidance should be considered alongside our Policy Statement on Prudential Regime for Cryptoasssets (PS 26/12).

How it links to our objectives

1.13 This guidance builds on PS 26/12. The rationale for how our rules, which we previously consulted on, link to our objectives remains relevant. This guidance aligns with our primary objectives of consumer protection, market integrity, and effective competition and also advances our secondary objective to promote international competitiveness and growth, as far as reasonably possible.

Environmental, social and governance considerations

1.14 In developing this GC, we have considered the environmental, social and governance (ESG) implications of our proposals and our duty under ss. 1B(5) and 3B(1)(c) of the Financial Services and Markets Act 2000 (FSMA) to have regard to contributing towards the Secretary of State achieving compliance with the net-zero emissions target under s.1 of the Climate Change Act 2008 and environmental targets under s.5 of the Environment Act 2021. Overall, we do not consider that the proposals are relevant to contributing to those targets. We will keep this under review during the consultation period.

Equality and diversity considerations

1.15 We have considered the equality and diversity issues that may arise from the proposals in this GC.

1.16 Overall, we do not consider that the proposals materially impact any of the groups with protected characteristics under the Equality Act 2010 (in Northern Ireland, the Equality Act is not enacted but other antidiscrimination legislation applies).

1.17 We will continue to consider the equality and diversity implications of the proposals during the consultation period and will revisit them when issuing the final guidance. In the meantime, we welcome your input on the issues raised in this GC.

Costs and benefits of our proposals

1.18 Section 138I of FSMA requires us to perform a cost benefit analysis for new rules but not for guidance (see s.139A of FSMA on power of the FCA to give guidance and s.139B of FSMA on the meaning of general guidance).

1.19 However, it is our policy to produce a Cost Benefit Analysis (CBA) for general guidance about rules if a high-level assessment of the impact of the proposal identifies an element of novelty, which may be in effect prescriptive or prohibitive, that may result in significant costs being incurred.

1.20 In this case, the proposed guidance seeks to clarify the incoming rules, as well as FCA Principles, rather than establish new policy. Therefore, the proposed guidance is not expected to result in materially different costs or benefits.

Next steps

1.21 The consultation period will run from 30 June 2026 until 30 July 2026. During this time, the FCA will be seeking feedback on the draft guidance.

1.22 Following the end of the consultation period, we will update the draft guidance to reflect feedback from stakeholders. We plan to publish the non-handbook guidance by 30 September 2026.

How to respond

1.23 Please review the proposals outlined in this guidance. We are seeking your views on the content of the proposed guidance in Annex 1 in particular the questions listed in Chapter 2.

1.24 We welcome responses by 30 July 2026. Where respondents do not agree with our proposed guidance, we would welcome further detail on their concerns and potential solutions.

1.25 You can send us your comments using the form on our website or by email to gc26-5@fca.org.uk. If responding by email, please indicate whether you wish your response to be treated as confidential, and separately, if you are content to be named as a respondent.

2 Consultation Questions

Q1: Does the proposed guidance clarify the prudential rules in CRYPTOPRU 7? If not, what more could we do to provide clarity?

Q2: Do you have any comments on the proposed guidance including the examples given?

Annex 1: Draft non-Handbook Guidance on CRYPTOPRU 7: Overall risk assessment for CRYPTOPRU firms

1. Introduction

1.1 We are issuing this general guidance (Guidance) under section 139A of the Financial Services and Markets Act 2000 (FSMA). It provides guidance to firms on how they should comply with their obligations under CRYPTOPRU 7 (Overall risk assessment).

1.2 The obligation for relevant firms to complete an overall risk assessment is set out in COREPRU 7. Firms should refer to GC 26/4: Non-Handbook Guidance for COREPRU 7: Overall risk assessment, which provides a broader discussion of the elements of the overall risk assessment which is also relevant for CRYPOPRU firms. CRYPTOPRU 7 contains provisions on what CRYPTOPRU firms specifically should include in their assessment. This guidance should be read in conjunction with CRYPTOPRU 7 and is intended to help these firms develop their own assessments, calculate financial resource requirements and understand the implications of their wind down plan.

1.3 There is a wide range of business models captured by CRYPTOPRU and aspects of this Guidance will not be equally relevant to all. Firms should consider the relevance of this guidance to their own business, bearing in mind the nature of their activities. It is also important that they apply this guidance, where relevant, in a way that is proportionate to the scale and complexity of their activities.

1.4 This Guidance does not replace applicable rules, guidance or law and should always be interpreted in ways that are compatible with any legal or regulatory requirements.

1.5 This Guidance also builds on the following FCA guidance:

a. Finalised Guidance, FG20/1 (Our framework: assessing adequate financial resources)

b. The Wind-down Planning Guide.

1.6 It should be read in conjunction with any other guidance specific to the prudential sourcebook that applies to the firm.

2. CRYPTOPRU 7.2: Overall Risk Assessment: Risk Identification, Stress Testing, Recovery Actions and Wind Down Planning.

This section refers to CRYPTOPRU 7.2.1R (2) Risk Appetite

2.1. A firm's overall risk assessment should begin with a clear understanding of its business model and strategy. This should cover the firm's main activities and the core underlying assumptions behind its business plan. A firm should consider how it expects to generate returns and the key vulnerabilities that could affect its ability to continue operating. The assessment should identify risks that may cause material harm and consider how changes in the firm's operations or in the wider business environment could change or increase those risks. The assessment should be forward-looking and reflect both the firm's current position and its expected future position, including the effect of proposed decisions such as new products, new business lines, growth plans or material operating changes. This identification of risk should include exposure risk, arising directly from balance sheet positions and transactions, and risk arising from the activities undertaken in pursuit of the business model (operational risk).

2.2. In considering the risks relating to assets on the balance sheet a firm should have regard to the risks associated with contractual and non-contractual features of that asset type. For example, where a firm holds tokenised assets, it should consider whether there are specific risks affecting the realisability or liquidity of those assets.

Examples of the risks that may be relevant for CRYPTOPRU firms include:

- Market risk - losses arising from changes in the value of assets, whether those values are directly observable in a market or modelled. For example, a firm that trades cryptoasset positions as principal may be exposed to changes in value.
- Leverage - leveraged positions that may increase sensitivity to market sell-offs and volatility.
- Credit risk - the failure of a counterparty in a financial transaction that may lead directly to loss, including where funds or assets are held in prefunded trading venues.
- Liquidity risk - not having enough cash or liquid assets to meet obligations as they fall due. This includes predictable and less predictable contractual or non-contractual obligations, timing mismatches between inflows and outflows, increased margin requirements under stressed conditions, and the availability of cash or other liquid assets that can be used when needed.
- Operational risk - loss resulting from inadequate or failed internal processes, people and systems or from external events.

- Market liquidity - assets becoming difficult to sell or only able to be sold at a significant discount to the market price. This may arise from shallow markets, concentrations, undisclosed connections between counterparties, or stress-driven behaviour of market participants.
- Concentration risk - the risk arising from a lack of diversification across assets, counterparties, income sources, service providers, custody arrangements or other exposures. Heavy reliance on a single asset, exchange, financial partner or operational dependency can increase vulnerability.

This section refers to CRYPTOPRU 7.2.1R (3) Risk Mitigation

2.3. As part of its overall risk assessment a firm should consider how it can reduce the risks from its activities. Risk should first be addressed through systems and controls that identify how harm may arise and how it can be avoided or reduced. Other mitigants are also relevant, such as collateral, committed facilities or operational contingency arrangements. In all cases, firms should consider how reliable those mitigants are and whether they continue to be effective under stress. Where mitigants are insufficient or unreliable, firms should consider holding additional financial resources as a way of mitigating the remaining risk. If, after these measures, the risk remains outside the firm's risk appetite, the firm should consider whether it should continue the activity that gives rise to that risk.

2.4. Having identified the risks that are relevant and understood the effectiveness of the ways those risks are mitigated, a firm should set its risk appetite. This is the overarching level of risk that a firm is willing to accept to generate acceptable returns. This should be allocated across the risks identified, and be proportionate to the nature, scale and complexity of its business model and organisational structure. It should be informed by regulatory and any other requirements that would affect the firm's ability to continue its activities and represents the degree of certainty that the firm will continue in business that is acceptable to the management body.

2.5. The risk appetite takes effect through a range of limits, tolerances, early warning indicators and triggers for action that ensure that the risks incurred do not exceed the appetite stated. In practice, this requires monitoring and reporting against metrics that show the level of the different risks that arise from the assets the firm owns and the activities it undertakes. A well-designed framework helps the firm decide when to strengthen controls, when to take recovery action, and when more significant action may be needed, including actions linked to wind-down planning.

This section refers to CRYPTOPRU 7.2.1R (4) Forward looking basis of assessment

2.6. When carrying out its overall risk assessment, a firm should take a forward-looking view of its business activities and of developments in the wider environment that could affect it. This includes considering how economic, market, operational or geopolitical developments could affect the risks from its activities that may cause material harm, and how those changes could

affect the amount and quality of own funds and liquid assets needed to meet the overall financial adequacy rule. The firm should consider both changes in the amount of financial resources required and changes in the quality, availability or reliability of those resources.

This section refers to CRYPTOPRU 7.2.1R (5) Severe but plausible stresses

2.7. Stress testing is critical to the development of an overall risk assessment and is used in a variety of ways. In assessing adequate financial resources, a firm should understand how its risks, mitigants and financial resources behave in both business-as-usual conditions and under stress.

2.8. Stress tests should include severe. In historical terms this means that stresses applied should not use metrics that are less severe than those already observed over an appropriate timeframe. Firms should also consider the potential for stress events, or degrees of stress, to occur that are more severe than those yet observed. This is particularly relevant in sectors without a relatively long history such as cryptoassets. Stress tests should also be plausible. In general, stresses should start with the risks that firms monitor and report. Stresses should also be consistent with firm's risk appetite as described below.

2.9. Firms should consider risks that may stop them putting things right when they go wrong as market participants can make mistakes or act in bad faith. The assessment of adequate financial resources should identify risks of potential harm to consumers and to markets and estimate their impact. This includes assessing the impact of any redress payable which may lead to financial stress and the potential depletion of financial resources including the inability to convert assets into cash in time to pay such obligations as they fall due.

Using stress testing to assess threshold requirements

2.10. Firms should use stress tests to assess the financial impact of a range of severe stress events on their business. This then informs the amount of own funds or liquid assets that is identified as the own funds threshold requirement and the liquid assets threshold requirement. The stresses applied should be consistent with the stated risk appetite for the severity of event that the firm wants to be able to survive. Firms should look at the range of relevant stresses and use both market wide stress events and firm specific events to test the impact on financial resources. Losses that could arise from balance sheet exposures should be considered as well as scenarios relating to potential operational issues and failures.

Using stress testing to assess resources held above threshold requirements

2.11. A firm should apply relevant stresses to its business model and the wider economic environment to assess whether the financial resources it holds above its threshold requirements are enough to absorb the impact of

relevant downturns while continuing to meet threshold requirements. This should inform the firm's risk appetite, trigger points and recovery actions.

Using reverse stress testing to support recovery and wind-down planning

2.12. A reverse stress test is intended to identify the point at which a firm's business model stops being viable. This therefore implies a scenario that is more severe than is envisaged by the firm's risk appetite. It should inform recovery planning and wind-down planning, including the setting of triggers for the decision to wind down such that the firm has sufficient own funds and liquid assets at the point the decision is taken to begin an orderly wind down.

Design and use of stress testing and scenario analysis

2.13. Stress tests and scenario analysis should be relevant to the firm's business model and the markets in which it operates. Scenarios should be forward-looking, severe but plausible, and based on clear, internally consistent assumptions. They may draw on historic events, hypothetical future events, or both. A firm should consider firm-specific and market-wide stresses, separately and in combination, and, where relevant, at the level of material business lines or portfolios as well as at a firm-wide level. The aim is to improve the firm's understanding of where losses, liquidity pressure or operational strain could arise and how these could affect the firm's viability.

2.14. A firm should identify adverse circumstances of different types, severity and duration, including circumstances developing over a prolonged period, sudden and severe events, and combinations of both. Stress testing programmes should be reviewed regularly to ensure they remain relevant. Firms should also use stress testing to assess the impact of material specific changes such as acquisitions or disposals of business units. The following are examples of the different types of stress:

- **Firm-specific stresses:** a targeted cyber-attack leading to the loss or theft of private keys; sudden unavailability of individuals with access to critical cold storage; or the failure of a principal trading partner or exchange where the firm holds material balances.
- **Market-wide stresses:** rapid and significant declines in cryptoasset prices leading to losses and widespread withdrawals by customers; loss of confidence in a qualifying stablecoin affecting firms that rely on it for collateral or liquidity management; or sudden withdrawal of liquidity across trading venues, making positions hard to unwind without material loss.
- **Combined stresses:** a major market sell-off occurring at the same time as a cyber incident affecting firm-held assets; or a series of defaults among exchanges and trading venues, triggered by the failure of a large

counterparty and worsened by sector-wide reliance on the same assets or collateral.

Examples of own funds stress factors

The list below contains examples of stress factors that may be relevant. It is not exhaustive and should be tailored to be appropriate to a firm given the nature and scale of its business.

- **Credit Risk:** creditors may default on amounts owed. This may be exacerbated by collateral backing a loan becoming insufficient to cover the outstanding debt as a result of market movements.
- **Market Risk:** cryptoassets may fluctuate significantly in value and firms are unable to deal at the rate quoted to the client resulting in losses for the firm.
- **Concentration Risk (can have both liquidity and capital implications):**
    - failure of a significant counterparty leads to a liquidity shortfall that causes the firm to default on its own obligations;
    - difficulty moving to another counterparty leads to cessation of operations; or
    - concentrations in tokens, protocols or counterparties increase the impact of stress.
- **Operational Risk:**
    - Internal fraud:
        - Mismarking of position to artificially inflate the value of crypto assets held.
        - Theft of proprietary code
    - External fraud:
        - Market manipulation attacks designed to exploit matching and pricing algorithms. The manipulator submits and then cancels large buy orders to increase prices and then capitalises on this movement by selling at the artificially higher price.
    - Employment practices and workplace safety
        - Discrimination, termination issues
        - Large numbers of staff absent due to illness during a pandemic.
    - Clients, products and business practices
        - Firm commences trading in products without the necessary regulatory permissions.
        - Anti-money laundering / Counter terrorist finance systems allow use of privacy coins that obscure ownership leading to accounts being used for unethical purposes.
        - Failed Customer Due Diligence: Opening accounts for shell companies without identifying the ultimate beneficial owner or accepting inconsistent identification documents.
        - Bypassing Know Your Customer controls to accelerate client onboarding or offering products without adequate money laundering risk assessments

        - Inadequate transaction monitoring not identifying source of funds or beneficiary/recipient.
    - Damage to physical assets:
        - Main office or building housing core technology is flooded and unusable for a period of time.
    - Business disruption and system failures:
        - Cyber-attack results in the firm being unable to access systems and provide services for 3 weeks. This results in loss of revenue, a liquidity shortfall and fines from regulators. Upon resuming service, over 50% of customers move their assets/transactions to a different provider making the business no longer viable.
    - Execution, delivery and process management:
        - Failed trade settlement and reconciliation: Inaccurate recording of crypto-asset holdings between a custodian and the actual blockchain, leading to broken trades.
        - Irrevocable Transaction Errors: a "fat-finger" error (entering an incorrect amount or destination address) by a user or staff member results in immediate and irreversible loss.
        - Key Mismanagement: Losing or misplacing the private keys to a cold storage wallet, resulting in the permanent inability to access or move crypto-assets.
        - Large numbers of outsourced providers are absent due to illness during a pandemic

Reverse Stress Test

The following are examples of reverse stress test scenarios that may be relevant:

- A systems related event has a prolonged impact stopping a bank from processing all transactions including withdrawals from both operational bank accounts and bank accounts forming part of the backing asset pool for issued stablecoins.
- A cyber-attack prevents the firm from accessing systems and providing services for an extended period, causing loss of revenue, a liquidity shortfall and regulatory costs, followed by a large outflow of customers that makes the business no longer viable.
- The market loses confidence in a firm, resulting in the loss of a substantial portion of counterparties or clients leading to the business becoming no longer viable.
- Complications arising because of material dependencies on group entities (e.g. services, funding, reputation, etc) becoming no longer available leading to the business being no longer viable.
- Existing shareholders are unwilling to provide new capital/investment to a loss- making firm making the business no longer viable.

This section refers to CRYPTOPRU 7.2.3R Recovery Actions

2.15. As part of its framework for managing risks and financial resources, a firm should consider and identify options available to management when the

business plan is not delivering the expected outcome. In particular, firms should consider the actions they could take when the levels of financial resource are trending downwards and there is a risk that the firm will no longer be able to meet their own funds threshold requirement or liquid assets threshold requirement. In cases where a firm's own wind-down trigger is materially lower than the threshold requirements, firms should also consider whether there are recovery actions which might still be available to them, after the breach of threshold requirements, that would enable them to avoid wind down and restore their financial position within the time available.

2.16. When considering potential recovery actions, a firm should identify a range of measures. Particular attention should be paid to anything that might prevent action being taken, how long it would take to initiate the action and the length of time needed for the action to take effect. These factors should help identify the point at which the action needs to be taken to be effective. As a result, these actions will be clearly defined, within the control of management, linked to internal triggers, and capable of timely implementation. Such actions could include improving the liquidity position; asking shareholders to inject more capital; taking steps to reduce the likelihood of further foreseeable losses materialising, for example by restructuring the business; and adjusting risk exposures, for example by changing the firm's business profile and business model.

2.17. A firm should understand the total impact of the recovery actions available to it during different forms of stress and reflect this in its assessment of financial resilience. A firm with few credible recovery actions is more vulnerable to financial stress, and that should be reflected in its assessment of trigger levels, recovery capacity and the point at which wind-down action may be needed.

2.18. Firms should have a contingency funding plan (CFP). This could be a part of an overall recovery plan document or a separate document that is integrated with recovery planning. An operable CFP is also an important part of a liquidity risk management framework. A CFP will typically have a named individual with delegated authority from the board who can choose from a list of actions preapproved by the board. While CFPs will vary significantly in proportion with the nature, scale and complexity of the underlying business, in practice a CFP should:

- set clearly defined quantitative internal action triggers above relevant threshold levels and by reference to the firm's risk appetite
- cover actions that may raise liquidity, such as drawdowns, repos or asset sales, and also actions that may conserve liquidity, such as reducing limits or requiring client pre-funding
- identify the range of credible contingency actions
- test the operability of contingency actions under business-as-usual conditions so that the firm understands whether they can be executed quickly and effectively in stress
- be integrated with stressed cashflow forecasting, severe-but-plausible stress scenarios and forward-looking liquidity analysis
- ensure appropriately granular liquidity analysis recognising that many firms face most of their liquidity outflows within the first 1–2 days of a stress event

- cover internal and external communications

2.19. Firms with a limited liquidity risk profile and a simple management structure may not have extensive contingency plans. However, it is still important to recognise that options are limited and ensure that this is reflected in both stress testing and when considering wind down triggers.

This section refers to CRYPTOPRU 7.2.6R Wind down planning

2.20. A firm must assess the financial resources it needs to exit the market without causing material harm. This assessment should identify the operational, financial and liquidity needs that may arise during wind-down. At a minimum, the firm should consider anticipated reductions in revenue, additional costs of closing operations, such as the cost of distributing custody assets or unwinding the stablecoin backing assets, and obligations that must continue to be met during wind-down. The analysis should be tailored to the firm's activities, risks and dependencies, and should consider how customers, counterparties, funding providers and third-party suppliers may behave once wind-down begins. A sufficiently detailed wind-down analysis supports credible execution under stress and a more reliable estimate of the resources required. Further guidance can be found in TR22/1: Observations on wind-down planning: liquidity, triggers & intragroup dependencies.

2.21. As a starting point for wind-down planning, a firm should consider:

- producing a list of all contractual relationships including contracts of employment
- extracting the termination / break clauses, notice periods, and exit penalties within each contract
- identifying the interdependencies and interrelationships between these contracts

2.22. The combination of this data should help to determine the appropriate timelines for exiting these contractual relationships during the wind-down process.

2.23. The above analysis will support assumptions used to formulate projected financials during the wind-down process such as, projected peak liquidity requirements, overall own funds requirements, and staffing and operational levels that are an integral part of an operational wind-down plan. Successful completion of a wind-down process will require firms to be able to cope with peak liquidity outflows as they arise and also have an appropriate overall (net) level of own funds. In wind-down planning, projections of liquidity requirements and projected own funds requirements can be materially different.

3. CRYPTOPRU 7.3: Overall risk assessment: own funds

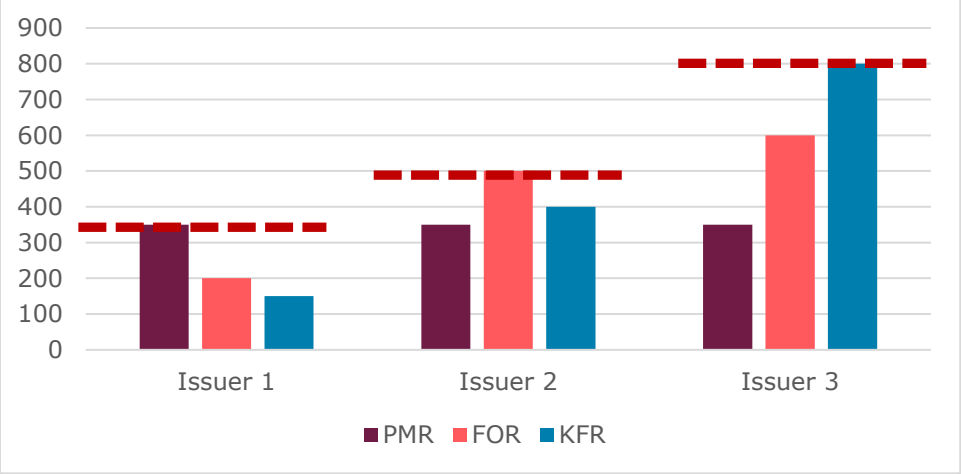
This section refers to CRYPTOPRU 7.3.2G Own Funds

Identifying minimum levels of own funds

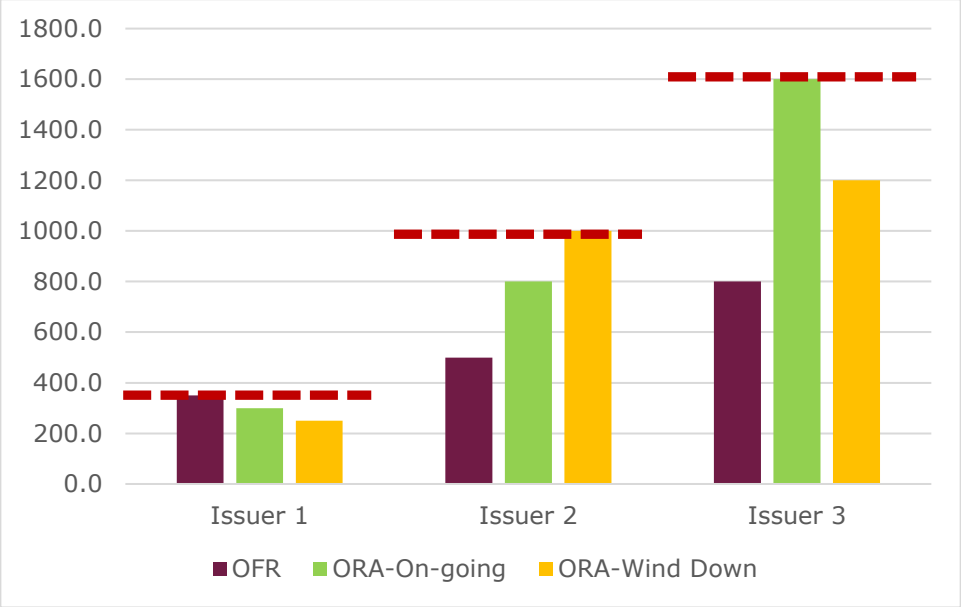
3.1. To meet the overall financial adequacy rule, firms must identify the minimum levels of own funds and liquid assets that are consistent with the rule (as set out in COREPRU 7.2.1R). These levels are known as the own funds threshold requirement and the liquid assets threshold requirement, respectively. Identifying the relevant levels involves 2 stages.

Own Funds

3.2. In stage 1, firms should calculate their own funds requirement (OFR) which is the higher of the permanent minimum requirement, the fixed overheads requirement and the K-factor requirement as set out in COREPRU 4. The OFR sets a floor for the own funds threshold requirement (OFTR). The diagram below illustrates how the OFR is determined for firms on each of the three distinct bases.



3.3. Stage 2 forms part of the overall risk assessment, in which firms are required to examine their own risks in the context of their own business model, counterparties, control frameworks and risk appetite. They use this process to identify the level of financial resources that is necessary to enable them to meet the overall financial adequacy rule at all times. There are two assessments required by the overall financial adequacy rule: the level required to remain financially viable through the economic cycle while still addressing material harm arising from activities, and the level required to enable the business to wind down without causing material harm. The higher of these two assessments is the own funds threshold requirement (OFTR) but, as noted above, it cannot be lower than the own funds requirement (OFR) calculated in stage 1. This is illustrated in the diagram below showing the different bases for the OFTR.



This section refers to CRYPTOPRU 7.3.3R Own Funds Threshold Requirement

3.4. A firm should ensure that the own funds it uses to meet its own funds threshold requirement satisfy the proportions in CRYPTOPRU 7.3.3R. Firms should also refer to COREPRU 3 for further detail on what qualifies as own funds.

CRYPTOPRU 7.4: Overall risk assessment: liquid assets

This section refers to CRYPTOPRU 7.4.2R Liquid Assets

4.1 To assess its liquidity needs over the next 90 days a firm should use a projection of both outflows and inflows of cash and liquid assets across time. Some flows can be projected with a high degree of precision while others will be estimates informed by expected levels of business. The projection should include reference to the current level of liquid assets and additional sources of cash available to the firm such as bank overdrafts, term loans, creditors and own funds. Having completed the projection on a contractual or expected basis firms should produce a stressed version. Elements that should be stressed are inflows being smaller than expected or delayed significantly, outflows being greater than expected and funding not being available on a timely basis or withdrawn altogether. Firms should also consider a reduction in market liquidity such that currently liquid assets are unable to be turned into cash without significant loss of value. The shortfall in the stressed cashflow indicates the amount of liquid assets the firm needs in relation to the next 90 days. Firms should consider this both on a peak and cumulative basis.

4.2. When developing its 90-day cashflow forecast a firm should consider the following:

- estimating next-day peak business-as-usual liquidity needs;

- building the forecast using a broad range of operational inputs and behavioural analysis covering clients, counterparties and liquidity providers;
- estimating peak potential outflows from margin calls, settlement failures or increased settlement requirements, client drawdowns, pre-funding requirements.

4.3. In creating a stressed version of the 90-day forecast a firm should include:

- stresses to cash inflows both in terms of amount being smaller and timing being delayed
- outflows being larger than expected
- sources of funding not being available on a timely basis or being withdrawn altogether
- reductions in market liquidity such that assets cannot be turned into cash without significant loss of value

The purpose should be to produce outputs that support action. These may include identifying large next-day use of liquidity facilities, placing adequate liquidity in relevant operational bank or clearing accounts to meet foreseeable outflows, and identifying large open positions and settlement dependencies.

4.4. The firm should update the methodologies and assumptions used in its 90-day stressed cashflow forecast following any material change to its business model or operating model. It should also carry out periodic back-testing to assess whether its stressed cashflow forecasts accurately reflect actual stressed cashflows experienced by the firm. The complexity and frequency of the forecast should be proportionate to the business activities of the firm, its overall liquidity risk profile and the risk of harm. Firms with highly predictable cashflows may be able to roll the analysis forwards with only periodic checks to ensure it remains relevant. Firms with more volatile flows may need to update projections to reflect activity as often as daily to ensure they can calculate their liquidity needs on a rolling basis

4.5. When estimating the liquid assets required for wind-down, a firm should consider the cashflow profile of its wind-down plan. This includes ongoing operational costs, settlement obligations, the return of assets to clients, and payments to creditors, including employees. The firm should identify and assess risks that may cause material harm during wind-down, such as market volatility affecting asset values, withdrawal of funding arrangements, and dependencies on group companies, and should ensure that enough liquid assets are available to manage those risks.

This section refers to CRYPTOPRU 7.4.3R Funding Profile

4.6. A firm's funding profile should consider the sources of funds that support its operations and the assets it holds, and the extent to which withdrawal or disruption of those funding sources could create an immediate need for liquid assets. A firm must take a forward-looking view of its funding profile

over the coming 12 months. This should include estimating funding needs in normal conditions and in stress, drawing on the 90-day stressed cashflow forecast to understand how liquidity and funding pressure may develop. The firm should consider the speed and severity with which funding stress could arise and how it may interact with the firm's business model and cashflow profile.

4.7. When reviewing funding sources, a firm must identify the significant funding arrangements on which it expects to rely over the next 12 months and assess the risks associated with renewing or rolling over those arrangements. The analysis should take account of possible constraints in stress, including withdrawal or unavailability of facilities, reduced access to group funding and changes in market conditions that increase the cost of funding. Different funding sources may behave differently in stress, and diversification of funding sources may help reduce these risks. Where funding gaps, or potential gaps, are identified a firm has opportunity to address those before they affect the rolling 90-day assessment and require additional liquid assets to be held.

This section refers to CRYPTOPRU 7.4.8R Liquid Asset Threshold Requirement

4.8. Firm may meet its liquid assets threshold requirement (LATR) by holding an appropriate combination of core and non-core liquid assets, provided those assets are of sufficient quality and can reliably meet liquidity needs as they arise. In deciding the composition of its liquid asset resources, the firm should ensure that liquid assets are not encumbered, are owned by the firm and are readily convertible into cash with minimal loss of value.

4.9. When assessing liquid asset levels, a firm should also consider whether an asset is operationally accessible in the required timeframe. For example, liquid assets held with a broker, prime broker, central clearing house, central counterparty or similar entity may be available to meet a liquidity need arising with that counterparty but may not be immediately transferable elsewhere. In those circumstances, the asset may be more appropriately treated as a mitigant to a specific liquidity requirement rather than as part of the firm's overall available liquid assets.

4.10. Similarly, available headroom on liquidity facilities does not count as a liquid asset; however, when preparing its 90-day business-as-usual and stressed cashflow forecast, this headroom can be recognised as a funding source that reduces liquidity requirements provided there are no contractual or operational restrictions that would impact their timely availability, such as cut-off times, lengthy or complicated drawdown approval processes, or specific restrictions on use of drawdowns from the facility (e.g. can only be used to issue new stable coins).

4.11. Non-core liquid assets may only be used to meet additional liquid resources required above the basic liquid asset requirement, and only where the firm has strong evidence that those assets would remain convertible into cash in stress. If certain non-core assets are less reliable under stress, the firm should apply higher haircuts or exclude them.

This section refers to CRYPTOPRU 7.4.9R Non-core Liquid Assets

4.12. When identifying assets that may qualify as non-core liquid assets, a firm should ensure that the assets genuinely support its ability to meet liquidity needs in both normal and stressed market conditions. Non-core liquid assets may include short-term deposits with eligible institutions, claims on multilateral development banks or international organisations, claims on third-country central banks or governments, and other financial instruments that can reasonably be expected to provide liquidity when required.

4.13. Assets should not be classified as non-core liquid assets if their use for liquidity purposes is restricted or uncertain. This includes assets that belong to clients or are encumbered, because restrictions on transfer or sale prevent those assets being used to meet the firm's own liquidity needs. Assets issued by the firm or its affiliated entities, except for permitted short-term deposits with affiliated credit institutions, should also be excluded because those assets may not provide reliable value or marketability in stress. When deciding whether an asset is suitable for inclusion, the firm should assess how easily it can be monetised in practice, including any legal or operational constraints, the likely loss on conversion to cash, currency convertibility and the ability to transfer the asset across group entities or jurisdictions where relevant. The firm should also consider how stressed market conditions could affect the availability and usability of non-core liquid assets, including market depth, counterparty reliability and any restrictions imposed by liquidity providers.

This section refers to CRYPTOPRU 7.4.10R Assets in the firm's name but belonging to a client and encumbered assets

4.14. A firm should ensure that, when deciding whether an asset qualifies as a liquid asset for prudential purposes, it accurately distinguishes between assets that belong to the firm and assets that belong to a client. Money or other property held under client asset arrangements may still belong to a client even if held in the firm's own name. Those assets cannot be relied on to meet the firm's own liquidity needs and should be excluded from the firm's liquid asset resources. The firm should also determine whether an asset is encumbered. An asset may be encumbered because it has been pledged as security or collateral, or because legal, regulatory, contractual or operational restrictions limit the firm's ability to liquidate, sell, transfer or assign it. Encumbered assets should not be counted towards liquid asset resources because the firm may not be able to convert them into cash when needed.

Example of encumbered asset balance sheet (qualifying stablecoin issuer)

4.15. This illustration shows how a firm may distinguish between total carrying amounts, encumbered assets and unencumbered assets. The purpose is to help a firm identify which assets may be available for liquidity purposes and which are not. Assets that are pledged, securitised, used as repo collateral, borrowed against or otherwise restricted should be treated as encumbered and should not be assumed to be available to meet the firm's own liquidity needs. Only the unencumbered portion should be considered available, subject to the relevant rules and any further assessment of liquidity and usability.

As of December 31, 202X

Asset Category	**Total Carrying Amount (A)**	**Encumbered Assets (B)**	**Unencumbered Assets (C)**
Cash & Cash Equivalents	£10M	£0	£10M
Debt Securities	£30M	£15M (Repo Collateral)	£15M
Equity Instruments	£5M	£2M (Borrowed)	£3M
Total Assets	**£45M**	**£17M**	**£28M**

This section refers to CRYPTOPRU 7.4.11R Applying haircuts to the value of non-core liquid assets

4.16. Guidance on the application of haircuts, including guidance on asset specific minimum haircut ranges, can be found in CRYPTOPRU 7.4.12G, 7.4.13G and 7.4.14G. In general, when determining an appropriate haircut for a non-core liquid asset, a firm should assess the potential loss of value that may arise when converting the asset into cash in stressed market conditions. The assessment should take account of legal, operational and market constraints that may delay or restrict monetisation. The firm should consider the asset's characteristics, including market depth, credit quality, currency denomination, and likely client and counterparty behaviour in periods of stress. The haircut should reflect the risk that the asset's value may fall materially before realisation.

4.17. The haircut should be calibrated using severe but plausible stress scenarios and reviewed regularly to ensure it remains appropriate as market conditions change. Assumptions about asset liquidity or price stability should be

conservative and supported by evidence from past stress events and current market indicators.

5. CRYPTOPRU 7.5: Overall Risk Assessment: review and document

This section refers to CRYPTOPRU 7.5.1R Overall Risk Assessment: Content

5.1. A firm's *overall risk assessment document* should clearly record the main judgements, assumptions and evidence supporting its assessment of financial adequacy. It should bring together the key parts of the *overall risk assessment* in a way that allows the firm, its *governing body* and the FCA to understand the firm's conclusions and the basis for them.

5.2. The document must include the matters listed in the rule. Where risks are not fully mitigated, it should record the implications for the firm's financial resilience. If matters are not documented, the firm may find it difficult to evidence, explain or defend its assessment.

This section refers to CRYPTOPRU 7.5.2R Governing Body

5.3. The governing body must take an active and informed role in overseeing the firm's overall risk assessment. It must review and approve the content of the overall risk assessment document within a timeframe that ensures the assessment remains current and reflects the firm's risk profile. The review should consider whether the assessment is proportionate to the nature, scale and complexity of the firm's activities and whether it properly identifies and evaluates the risks that may cause material harm.

5.4. The governing body must also review and approve the key assumptions that underpin the assessment. Those assumptions may relate to future conditions, business model vulnerabilities and potential stress events, and are fundamental to the firm's assessment of the adequacy of its financial resources. They should be supported by clear analysis, including stress testing where appropriate, and should take a forward-looking view of how risks may develop over time. The governing body's scrutiny is important to ensure that the assessment is robust, credible and used to support decision-making.

5.5. The governing body should ensure that it receives sufficient information about the firm's risk management framework, including how material risks are identified, the adequacy of systems and controls, and how risk assessment, stress testing and resource planning fit together. Where weaknesses or gaps are identified, the governing body should ensure that appropriate improvements are made and that any limitations in the assessment are understood before approval is given.

6. CRYPTOPRU 7.6 Overall risk assessment: firms forming part of a group

This section refers to CRYPTOPRU 7.6R Group Risk

6.1. A firm should ensure that its overall risk assessment gives proper consideration to the risks associated with group membership. These risks may include dependence on other group entities for funding, operational support, governance, decision-making or the provision of critical services. The firm should assess how those dependencies could affect its financial resilience, particularly where group entities may change their risk appetite, reduce available support or themselves experience financial or operational stress. The assessment should be forward-looking and should consider how group structures or dependencies could create risks that may cause material harm.

6.2. A firm should also assess whether group membership could hinder its ability to wind down individually without causing material harm. This includes considering whether group governance, shared services or other operational interdependencies could affect the timing or execution of wind-down, or the availability of critical resources needed to support it.

6.3. Where a firm is part of a group, its overall risk assessment must provide a clear and structured evaluation of group risks that may cause material harm. The firm should consider whether reliance on group entities for funding, shared services, operational support or critical systems creates vulnerabilities, especially in stress. It should also assess whether group-level decision-making, governance processes or resource allocation could constrain its ability to meet obligations, maintain adequate *own funds* or *liquid assets*, or respond effectively to emerging risks.

6.4. The assessment should also address the effect of group-wide stress events or changes in group strategy. For example, group entities may experience financial distress, reduce intra-group funding, change their risk appetite or controls, or make decisions that affect the timing or feasibility of the firm's own risk mitigation actions.

Examples of sources of group risk specific to CRYPTOPRU firms include:

- **Liquidity and peg stability risk for qualifying stablecoin issuers.** Sudden redemption surges or mass withdrawals may put pressure on liquidity and lead to peg deviation. Where reserve structures differ across subsidiaries or jurisdictions, liquidity stress in one part of the group may spread across the group. Joint or cross-border issuance arrangements may also fragment reserves and increase contagion risk.
- **Fragmented reserve custody risk for qualifying stablecoin issuers.** Different legal entities may manage reserves under different legal, regulatory or operational arrangements. Fragmentation across banks, custodians or protocols may increase operational and financial fragility.
- **Decentralised crypto exchange governance risk.** Where governance is spread across decentralised autonomous organisation arrangements, legal wrappers, development teams or operating entities, inconsistent controls or

concentrated influence may increase operational and financial risk across the group.

- **Technology dependency risk.** Inconsistent security standards across related entities may allow vulnerabilities in one part of the group to affect others, particularly where systems or contracts are interconnected.
- **Legal, jurisdictional and regulatory risk.** Multi-jurisdictional structures may create indirect financial exposures and legal uncertainty, including where different group entities perform different roles in a single cryptoasset business model.
- **Trading venue and cross-chain infrastructure risk.** Multiple blockchains, custody rails, bridges and settlement channels may increase fragmentation, interoperability risk and operational blind spots across group entities.
- **Crypto custodian group risk.** Centralised custody arrangements may create single points of failure for multiple group entities. Disruption in the custody entity may affect exchanges, brokers or other affiliated businesses that depend on it.
- **Crypto exchange traded products (ETP) group risk.** Where ETP are issued or supported by multiple group entities, volatility, liquidity strain, operational dependency or reserve asset stress in one entity may affect others, including through cross-border flows or market-making arrangements.