

# Finalised Guidance

## Non-Handbook guidance on CRYPTOPRU 7: Overall risk assessment for CRYPTOPRU firms

**FG 26/10**

September 2026

### 1 Introduction

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

Firms should read this in conjunction with CRYPTOPRU 7. It's intended to help them develop their own assessments, calculate financial resource requirements, and understand the implications of their wind-down plan.

- 1.2 CRYPTOPRU captures a wide range of business models, and not all aspects of this guidance will be relevant to all of them. Firms should consider it in the context of their own business and the nature of their activities and apply it in proportion to the scale and complexity of their activities.
- 1.3 This guidance does not replace applicable rules, other guidance or law and should always be interpreted in ways that are compatible with any legal or regulatory requirements. Its contents are illustrative and non-exhaustive, and do not prescribe a single methodology.
- 1.4 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.

- 1.5 It should be read in conjunction with any other guidance specific to the prudential sourcebook that applies to the firm.
- 1.6 The obligation for firms to complete an overall risk assessment is set out in COREPRU 7. Firms should refer to [FG26/9: Non-Handbook guidance for COREPRU 7: Overall risk assessment](#). This provides a broader discussion of the elements of the overall risk assessment, which is also relevant for CRYPTOPRU firms. CRYPTOPRU 7 contains provisions on what CRYPTOPRU firms specifically should include in their assessment.
- 1.7 This Guidance comes into force on 25 October 2027.

## 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 by understanding its business model and strategy. This should cover the firm’s main activities and the underlying assumptions of its business plan.

A firm should consider how it expects to generate returns, and the vulnerabilities that could affect its ability to operate. 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 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 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 balance sheet risks, a firm should consider 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 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** – risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
- **Combined risks** – such as market and liquidity risks, where assets become difficult to sell or only able to be sold at a significant discount to the market price though prices themselves may not have fallen. 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. It should first address this through systems and controls that identify how harm may arise, and how to avoid or reduce it. 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 remain effective under stress. If 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, it should consider whether to continue the activity that gives rise to that risk.

- 2.4 Having considered the above, a firm should set its risk appetite. This is the overarching level of risk that it 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 other requirements that affect the firm’s ability to continue its activities. It represents the degree of certainty that it will be able to continue operating that the management body finds acceptable.
- 2.5 The risk appetite takes effect through a range of limits, tolerances, early warning indicators, and triggers for action. These ensure that the risks incurred do not exceed the appetite. 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 initiating wind-down plans.

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 in their quality, availability and reliability.

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

- 2.7 Stress testing is critical to developing 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 but plausible stresses. In historical terms, this means that stresses applied should not use metrics that are less severe than those already observed over an appropriate timeframe.
- 2.9 There Firms should also consider potential stress events, or degrees of stress that are more severe than those already seen. This is particularly relevant in sectors without a long history such as cryptoassets. Stress tests should also be plausible. In general, stresses should start with the risks that firms monitor and report and be consistent with firm's risk appetite.
- 2.10 Firms should also factor in the uncertainty arising from the sector's limited track record, including uncertainty about banks' willingness to provide services and the lack of established legal precedent.
- 2.11 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, the potential depletion of financial resources, and the inability to convert assets into cash in time to pay such obligations as they fall due.

Using stress testing to assess threshold requirements

- 2.12 Firms should use stress tests to assess the financial impact of a range of severe stress events on the business. This will inform the amount of own funds or liquid assets it identifies 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.

Firms should consider losses that could arise from balance sheet exposures as well as scenarios relating to potential operational issues and failures.

Using stress testing to assess resources held above threshold requirements

- 2.13 A firm should apply stresses relevant 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 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

- 2.14 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 envisaged by the firm’s risk appetite. It should inform recovery planning and wind-down planning, including making sure that, at the point at which the decision is taken to wind down, the firm has sufficient own funds and liquid assets.

Design and use of stress testing and scenario analysis

- 2.15 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.

- 2.16 A firm should identify adverse circumstances of different types, severity and duration, including those developing over a long period, sudden and severe events, and combinations of both.

It should review its stress testing programmes regularly so that they remain relevant. Firms should also use stress testing to assess the impact of changes such as acquisitions or disposals of business units.

Here are some 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 data

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 the scale and nature of a firm’s business.

- **Credit risk:** Debtors or counterparties 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
  - concentrations in tokens, protocols or counterparties increase the impact of stress.
- **Operational risk:**
  - Internal fraud:
    - Mismatching 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
    - Key theft
  - 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 begins 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 cryptoasset 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 cryptoassets
  - Large numbers of outsourced providers are absent due to illness during a pandemic
  - Slashing events and correlated slashing due to client software faults across multiple validators, oracle failure or manipulation causing mispriced liquidations

### Reverse stress test

#### **Examples of reverse stress test scenarios:**

- A systems-related event has a prolonged impact stopping a banking counterparty 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**

- 2.17 As part of its framework for managing risks and financial resources, a firm should identify and consider options available to management when the business plan is not delivering the expected outcome.

In particular, the firm should consider the actions it could take when the levels of financial resource are trending downwards and there is a risk that it will no longer be able to meet its 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, it should also consider whether there are recovery actions available, after the breach of threshold requirements, that would allow it to avoid wind-down and restore its financial position within the time available.

- 2.18 When considering potential recovery actions, a firm should identify a range of measures. It should pay particular attention 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, so it can identify the point at which the action will be effective.

As a result, these actions will be clearly defined, within the control of management, linked to internal triggers, and capable of being implemented promptly.

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, such as changing the firm's business profile and business model.

- 2.19 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.
- 2.20 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 an important part of a liquidity risk management framework. It will typically have a named individual with delegated authority from the board who can choose from a list of actions it has preapproved.

CFPs will vary in proportion with the nature, scale and complexity of the underlying business, but should :

- set clearly defined quantitative internal action triggers above 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 a stress event
- be integrated with stressed cashflow forecasting, severe-but-plausible stress scenarios and forward-looking liquidity analysis
- contain 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

2.21 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 where options are limited and ensure that this is reflected in setting risk appetites, stress testing and when considering wind-down triggers.

**This section refers to CRYPTOPRU 7.2.6R wind-down planning**

2.22 A firm must assess the financial resources it needs to exit the market without causing material harm. It 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 it must continue to meet during wind-down.

It should tailor the analysis to the firm's activities, risks and dependencies, and 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 is in TR22/1: Observations on wind-down planning: liquidity, triggers & intragroup dependencies.

2.23 Firms should recognise the particular risks they may face in a wind-down and assess whether they need additional resources. For example, cryptoasset custodians and custodial staking firms should take account of unbonding periods and withdrawal delays, which may extend materially in stressed market conditions.

Firms should also recognise the potentially significant on-chain transfer costs associated with returning assets to large numbers of clients, (particularly where

network fees rise sharply during periods of congestion or market stress), and the need for robust, documented and tested procedures for the secure handover of cryptographic keys or key shards during wind-down.

These procedures should include governance, segregation of duties, multi-party authorisation, audit trails and staffing arrangements to preserve the confidentiality, integrity and availability of client access mechanisms.

2.24 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

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

2.26 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 overall (net) level of own funds. In wind-down planning, projections of liquidity requirements and projected own funds requirements can be different.

### 3 CRYPTOPRU 7.3: Overall risk assessment: own funds

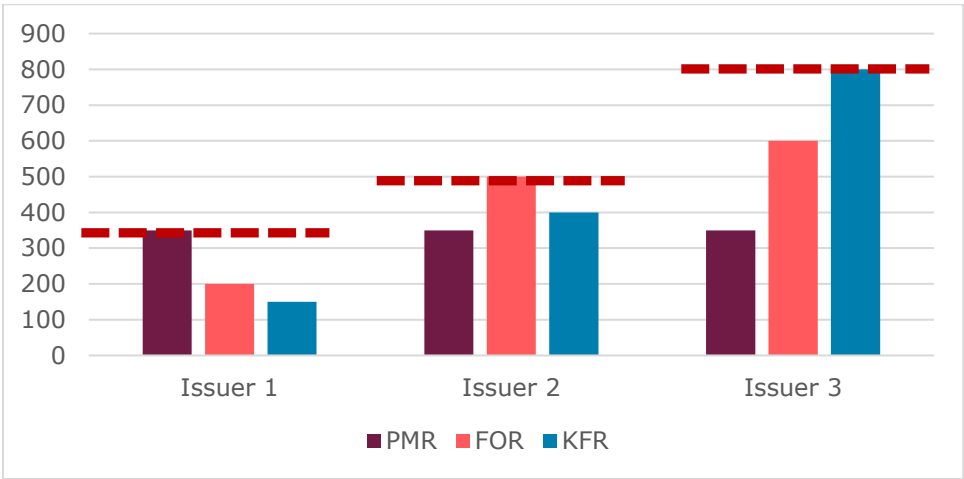
This section refers to CRYPTOPRU 7.3.2G own funds

#### 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 levels involves 2 stages.

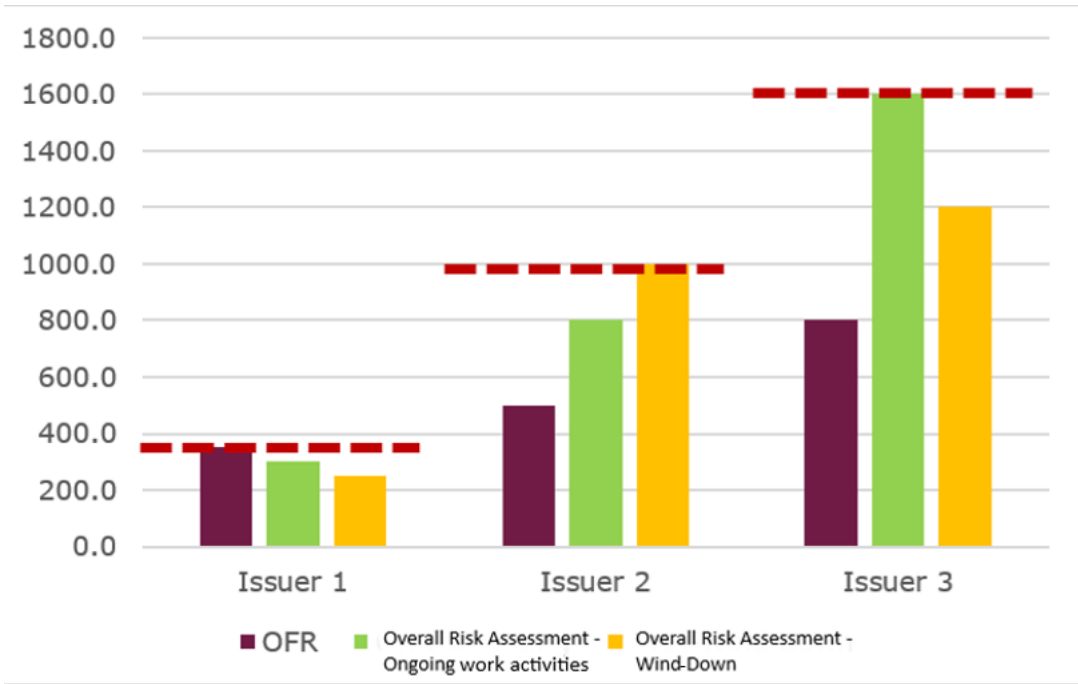
#### Own funds

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 3 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. CRYPTOPRU 7 refers to Assessment 'A' (on-going) and Assessment 'B' (wind down) for OFTR (CRYPTOPRU 7.3.2G) and LATR (CRYPTOPRU 7.4.5 G).

These are 2 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 2 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.

## 4. 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 precisely 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 facilities and capital sources.

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 happening sooner than anticipated 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:
- estimating 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

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

- stresses to cash inflows both in terms of smaller amounts or delayed timing
- outflows being larger, and happening earlier, 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 operational bank or clearing accounts to meet foreseeable outflows, and identifying large open positions and settlement dependencies.

- 4.3. 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 it experienced. The complexity and frequency of the forecast should be proportionate to the firm’s business activities, 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.

- 4.4. 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 dependence on group companies.

The firm should ensure that enough liquid assets are available to manage those risks.

**This section refers to CRYPTOPRU 7.4.3R funding profile**

- 4.5. 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 look at its funding profile for 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.

- 4.6. 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 them over.

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 diversifying 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 liquidity assessment and require it to hold additional liquid assets.

This section refers to CRYPTOPRU 7.4.8R liquid asset threshold requirement

- 4.7. A firm may meet its liquid assets threshold requirement (LATR) by holding a 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.

- 4.8. 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 not immediately transferable elsewhere.

In those circumstances, the asset may be better treated as a mitigant to a specific liquidity requirement rather than as part of the firm's overall available liquid assets.

- 4.9. Similarly, available headroom on liquidity facilities does not count as a liquid asset but when preparing its 90-day business-as-usual and stressed cashflow forecast, the firm may be able to recognise this headroom as a liquidity resource that reduces liquidity requirements.

It would need to ensure that there are no contractual or operational restrictions to this headroom, such as cut-off times, lengthy or complicated drawdown approval processes, or specific restrictions on use of drawdowns from the facility (e.g. it can only be used to issue new stablecoins).

Having done this, a firm should be able to assess the effectiveness of the facility in reducing the liquidity requirement and adjust appropriately.

- 4.10. Non-core liquid assets may only be used to meet additional liquid resources required above the basic liquid assets requirement (BLAR), 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

- 4.11. 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 provide liquidity when required.

- 4.12. 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 they 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.

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**

- 4.13. 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 the firm should exclude them from its liquid asset resources.

It 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)**

- 4.14. This illustration shows how a firm may distinguish between total carrying amounts, encumbered assets and unencumbered assets, to help it 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 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         |
| <b>Total Assets</b>     | <b>£45m</b> | <b>£17m</b>            | <b>£28m</b> |

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

- 4.15. 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 a 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.

- 4.16. 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 us to understand its conclusions and the

basis for them.

- 5.2. The document must include the matters listed in the rule. Where it hasn't fully mitigated risks, the firm should record the implications for its 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 how the firm assesses how adequate its financial resources are.

The assumptions should be supported by clear analysis, including stress testing, and evaluate how risks may develop over time. The governing body's scrutiny is important to ensure that the assessment is robust, credible and supports 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.

The governing body should ensure that improvements are made to any weaknesses or gaps, and that any limitations in the assessment are understood before they approve it.

## 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 properly considers the risks associated with group membership.

These 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 change their risk appetite, reduce available support or themselves experience financial or operational stress.

The assessment should be forward-looking and 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 resources 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 prevent it from meeting its obligations, maintaining adequate own funds or liquid assets, or responding to 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:**

- **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 rest of 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 governance risk.** Where governance is spread across decentralised autonomous organisational 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.

# Annex 1 Feedback statement

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

**Date of Consultation: 30 June 2026**

### Summary

---

1. This Non-Handbook guidance (NHG) is not exhaustive and is not a complete description of the steps firms should take when completing their overall risk assessment. It supports the prudential rules published in PS26/12 and in the FCA Handbook.
2. In June 2026, we consulted on the proposed Non-Handbook guidance on CRYPTOPRU 7: Overall risk assessment for CRYPTOPRU firms.
3. We received 11 responses mostly from cryptoassets firms, cryptoassets membership bodies and professional advisers. We can't respond to every comment individually, but this feedback statement summarises the points they made. We give a list of the non-confidential respondents at Annex 2.
4. We are now publishing a final edition of 'Non-Handbook guidance on CRYPTOPRU 7: Overall risk assessment for CRYPTOPRU firms.' This statement explains how we have considered the consultation feedback and taken it into account in our guidance.
5. We have decided to implement most of our original proposals but have made modifications in some areas to provide more clarity.
6. Two respondents shared their feedback on this consultation and on our concurrent consultation, '[GC26/4: Non-Handbook guidance on COREPRU 7: Overall risk assessment](#)' in a single document. Feedback specific to this consultation is addressed here. Feedback on broader prudential rules are addressed in '[FG26/9, the Finalised Non-Handbook guidance on COREPRU 7: Overall risk assessment](#)'. Respondents should refer to the relevant publication.

### Responses to feedback

7. We asked the following questions:  

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

### Key feedback themes

8. Most respondents welcomed the proposal. They recognised that the clarifications in GC26/5 set out our expectations for firms to consider when completing their overall risk assessment in a practical and logical way. Respondents also asked for clarification on:
- policy clarifications on general items
  - proportionality
  - additional detailed guidance

**Policy clarifications on general items**

9. One respondent highlighted a perceived ambiguity about the assessment of one of the K-factors, i.e. K-factor for Cryptoassets Safeguarded (K-RCS) and whether it should capture the operational surplus. They asked whether including the operational surplus in the K-RCS calculation could result in a double count in the capital requirement.
10. One respondent highlighted the importance of the conversion methodology applied to crypto-denominated balance sheets and revenue statements. They asked us to require firms to follow the provisions of CRYPTOPRU 4.12 for completing their overall risk assessment.
11. A respondent asked for further clarification on the future coverage of CRYPTOPRU, COREPRU and MIFIDPRU.
12. Two respondents asked for further clarification on the interaction with the Bank of England’s systemic stablecoin regime. This regime will not apply for the majority of our firms, but we recognise the point made that future collaboration may be beneficial.
13. Two respondents asked for further guidance on the consolidated overview of the prudential framework, citing that the requirements and expectations are currently distributed across [FG20/1](#), COREPRU, CRYPTOPRU, [FG 26/9](#) and [FG26/10](#).
14. One respondent asked for clarification on the mechanics of calculating the firm-level liquidity requirement, particularly how the firm’s own liquidity assessment interacts with the stablecoin backing-asset regime.

**Response**

We have shared the feedback on general policy items beyond this guidance with the relevant FCA policy areas for consideration and possible future policy development.

Operational surplus and K-RCS

An operational surplus should be excluded from the calculation of K-RCS. The operational surplus should be classified under the trading book which would lead to it being in scope of K-NCP.

Functional currency conversion

For functional currency conversion, firms should have a consistent and prudent approach to converting crypto-denominated assets into functional currencies.

Handbook roadmap

We will consult when moving other types of regulated firms (e.g. those subject to MIFIDPRU) into COREPRU and finalise the approach through our usual governance procedures. This will include feedback received from consultation papers. We cannot currently pre-empt what may be the approach on the Internal Capital Adequacy and Risk Assessment (ICARA) process in MIFIDPRU 7.

Systemic stablecoin regime

The joint paper that set out Bank of England and the FCA’s approach to joint regulation of systemic stablecoin issuers was published on 30 June 2026. Firms should consider the overall risk assessment in its entirety while under the FCA regime and monitor the policy developments of the systemic stablecoin regime where relevant.

Prudential framework

FG 20/1 explains our expectations on holding adequate financial resources, expanding on the Threshold Condition and Principles for Businesses. It applies to all FCA solo-regulated firms.

COREPRU (in its current application) and CRYPTOPRU make these expectations specific to cryptoasset firms, setting out minimum capital and liquidity requirements for this sector. They also contain the requirement for firms assess their own risks, and their need for financial resources.

FG 26/9 and FG 26/10 accompany the relevant sections on the overall risk assessment in chapter 7 in the new prudential sourcebooks, COREPRU and CRYPTOPRU respectively. They are part of our wider strategy to make our rules more accessible by distinguishing supporting material from core Handbook content.

LATR assessment for a stablecoin issuer

For a stablecoin issuer, the LATR is the sum of the BLAR, the applicable issuer liquid assets requirement (ILAR), and the higher of:

- (i) the firm’s own assessment of the stressed ongoing business liquidity needs (based on a 90-day liquidity forecast); and
- (ii) the firm’s incremental wind-down liquidity requirements over and above the BLAR.

Under CRYPTOPRU 6.1.4R, a qualifying stablecoin issuer must calculate its ILAR based on the following assets in its backing asset pool:

- core backing assets, excluding on-demand deposits
- expanded backing assets.

The ILAR should in most circumstances be sufficient to ensure the firm can cope with redemptions. However, there can also be large and sudden ‘redemption surges’ and potentially operational issues, i.e. disruptions, affecting backing pool bank accounts which the firm must consider as part of its overall LATR assessment.

This should ensure that the stressed ongoing business liquidity needs part of the LATR calculation captures any eventualities leading to potential shortfalls not captured in the ILAR (backing asset pool) assessments or computations.

In summary, the LATR mapped to liquid assets should be covered as follows:

- BLAR – should be covered by core liquid assets
- ILAR – must be covered by the backing asset pool(s) in the form of core liquid assets
- Stressed ongoing business liquidity needs (plus incremental liquidity requirements where the wind-down liquidity needs are higher) – must be covered by a combination of core and non-core liquid assets based on the firm’s own assessment.

**Proportionality**

- 15.** One respondent emphasised the importance of proportionality in reflecting different level of risks arising from various business models and activities. The respondent suggested that the guidance could benefit from a concise, technology-neutral matrix based on the functional drivers of prudential risk.
- 16.** One respondent stated that they are mindful that some firms will be experiencing financial regulation for the first time. They asked that we acknowledge this and work collaboratively with firms as they develop their approaches.
- 17.** One respondent highlighted that the risk-based approach is appropriate. Cryptoasset firms vary considerably in size and complexity, so proportionality will help avoid unnecessary burdens while maintaining standards.

**Response**

We appreciate the request for greater clarity on the application of proportionality, as well as the suggestions for additional language to be included in the guidance.

However, our view is that proportionality, and how it is reflected in a firm’s assessment, is ultimately a matter for firms to determine using their own judgement. Firms should apply and develop the principles underpinning the overall risk assessment in a way that is aligned with their assessment of risks and how they manage their business.

**Additional detailed guidance**

- 18.** One respondent suggested a short schedule to show how the firm:
  - separately calculates the own funds and liquid assets needed for ongoing operation and wind-down
  - maps common assumptions and financial effects across those assessments, K-factors, haircuts, cashflow stresses and specific liquidity requirements

- applies the threshold mechanics and records any aggregation, correlation or diversification assumptions
- 19.** One respondent argued that the international groups should be able to reuse group methodologies, data, scenarios and control testing, accompanied by a focused UK legal-entity assessment. That assessment should identify the UK firm’s liabilities and exposures, the location and legal availability of resources, transfer constraints, and operational availability during correlated group stress. The UK governing body should own and challenge the conclusion and ensure its consistency with any group-wide wind-down plan.
- 20.** One respondent asked us to clarify that under the final rules qualifying cryptoassets that are not admitted to a UK qualifying trading platform, or that cannot be prudently valued, are fully deducted from own funds. The guidance should clarify the 2 consequences for the assessment: in wind-down planning such holdings should be assumed to have no realisable value unless the firm can evidence otherwise; and stress testing need not hold further capital against price risk on positions already fully deducted, as the deduction is itself the capital treatment.
- 21.** One respondent asked the guidance to cover financial crime, sanctions, fraud, operational resilience and third-party dependencies. Considering these together will strengthen resilience.
- 22.** Two respondents requested further clarification on business model calibration. The guidance already recognises that aspects of it will not be equally relevant to all firms, but that principle would be more useful if the guidance gave clearer examples of how assumptions change across different permission profiles and business models.
- 23.** Finally, one respondent suggested the guidance draw a clearer line between risk appetite, early-warning triggers, threshold conditions, recovery action and the wind-down decision.

**Response**

We acknowledge the suggestions that requested further additional guidance. We do not consider it appropriate to provide an exhaustive list, given the wide range of business models, activities and circumstances to which the requirements may apply. Nor do we consider it desirable to provide an indicative list that could inadvertently narrow firms’ thinking or encourage a mechanistic approach. Firms should instead exercise judgement in determining what is relevant to their own assessment.

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

- 24.** Respondents broadly welcome our use of examples, diagrams and practical illustrations in the guidance. They consider these helpful for explaining prudential concepts such as own funds, liquidity resources, baseline and threshold requirements, encumbered assets, and wind-down planning.
- 25.** Three respondents requested confirmation that the examples are illustrative, non-exhaustive and non-prescriptive. Firms should be able to adopt different methodologies, including the use of group data or proxies where historical

data is limited, justified by their business model, scale, complexity and risk profile, supported by evidence.

- 26.** Four respondents suggested additional examples of risks such as: de-banking risk, legal uncertainty, private-key failures, cyber incidents, cold storage, prefunded trading venues, smart contract exploits, correlated slashing, validator-exit scenarios, oracle failures, bridge exploits, chain congestion, stablecoin de-pegs, risks from continuous settlement models, liquid staking token risks, blockchain outages and cross-chain infrastructure failures.
- 27.** Several respondents recommended that liquidity guidance should go beyond balance sheet ownership or accounting encumbrance and focus on whether assets are legally, operationally and practically available when needed. They identify constraints such as wallet access, banking cut-offs, settlement channels, jurisdictional restrictions, counterparty limitations, transfer times and out-of-hours access. One suggested that the liquidity stresses can be better tiered to distinguish what is applicable, for instance, to traders as compared to stablecoin issuers.
- 28.** Four respondents asked for more detailed examples addressing qualifying stablecoin issuers, including redemption surges, access to reserve assets, payment-rail dependencies, custodian and bank reliance, residual holders and separation between backing assets and corporate wind-down resources. There was also a broader request for clearer treatment of client assets versus firm assets, including how client-asset return or transfer affects liquidity, wind-down timing and operational capability.
- 29.** Some respondents suggested including combined scenarios that also trace the full sequence from stress event to loss, cashflow impact, early-warning indicators, mitigants, recovery actions, threshold breaches and wind-down decisions. This was seen as especially important because cryptoasset firms may face linked stresses involving price falls, customer withdrawals, counterparty failure, de-pegs, reduced market depth, infrastructure outages and cyber events at the same time. One respondent recommended the inclusion of the use of on-chain metrics in early warning indicators.
- 30.** A few respondents recommended that recovery actions should be distinguished between those within management control and those dependent on external parties such as banks, shareholders, counterparties, buyers or group entities. They also note that contingency funding options for cryptoasset firms may be limited due to banking resistance, which should be reflected in stress testing and wind-down triggers. Several respondents recommend a worked wind-down example that distinguishes own-funds costs from peak liquidity needs and clarifies when recovery should give way to orderly wind-down. One recommended a greater emphasis on contingency funding plans.
- 31.** Respondents welcome group-risk examples but suggest further coverage of dependencies on group entities for blockchain infrastructure, node operation, RPC access, signing services, custody arrangements and cross-entity operational failures. At the same time, one respondent requested proportionate examples for simpler firms.

- 32.** A few respondents identified drafting improvements including those that would clarify credit risk, funding sources, and reverse stress testing. One respondent suggested the diagrams on 3.2 and 3.3 could be enhanced to bring these 2 sections together.

**Response**

The examples in the guidance intended to be illustrative, non-exhaustive, and non-prescriptive. They are to help firms identify and assess the risks and potential stresses relevant to their business models, activities and operations.

We welcome the broad range of additional examples and enhancements suggested. Although some of these may be helpful for some firms, not all are universally applicable. We have made some additions to the guidance to include risks that are more widely relevant, such as de-banking and legal risk, as well as selected examples of stress scenarios that help illustrate the complexity of the cryptoasset environment. (Please see the Summary of key changes to the guidance at the end of this Annex 1).

We have not included an end-to-end illustration showing how a loss might affect client assets, a firm’s resources, resource requirements and triggers for action. This is to avoid implying that there is a single path through which such events may evolve. We do not consider it necessary to expand our discussion on contingency funding planning, preferring to leave any further consideration to firms’ discretion.

We have taken on board the drafting corrections proposed and have amended the language where it could give rise to interpretive uncertainty, particularly in relation to credit risk, funding sources and reverse stress testing.

We have also retained the diagrams in sections 3.2 and 3.3, since clarity on the setting of baseline requirements and threshold requirements was specifically requested during our discussions with firms under PS 26/12. (Please see the Summary of key changes to the NHG at the end of this Annex 1).

## Summary of key changes to the GC26/5 Non-Handbook Guidance

---

| Topic                       | Change                                                                           |
|-----------------------------|----------------------------------------------------------------------------------|
| Additional Risk examples    | De-banking risk and legal risk examples added in paragraph 2.10.                 |
| Additional Stress Scenarios | Additional relevant stress scenarios have been added in paragraph 2.16 and 2.23. |

# Annex 2 : List of non-confidential respondents

This Annex lists the respondents to our consultation who consented to the publication of their names:

- 1. Circle Internet Financial
- 2. European Ethereum Institute
- 3. Mansi Birla
- 4. Volodymyr Holovachov