GBBC RESPONSE TO FCA GUIDANCE CONSULTATION GC26/5

Non-Handbook Guidance on CRYPTOPRU 7

Overall risk assessment for CRYPTOPRU firms

About Global Blockchain Business Council (GBBC)

GBBC is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

GBBC furthers adoption of digital technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chains, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), GBBC Digital Media, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).

Introductory remarks and general comments

GBBC appreciates the opportunity to respond and welcomes the FCA's effort to translate CRYPTOPRU 7 into practical, accessible guidance. The overall risk assessment will be an important part of the new regime: it connects a firm's business model and risk appetite with its financial resources, recovery options and ability to wind down without causing material harm.

GC26/5 would be most useful if it showed how firms move from identifying material harm and testing controls to setting resources and taking management decisions. This is particularly important for business models spanning continuous cryptoasset markets, banking and payment rails, and shared international infrastructure. A list of risks cannot show whether a financial effect has been captured once, twice or not at all.

We focus on a small number of schedules and worked examples, used alongside GC26/4. They should remain illustrative: a different methodology should be acceptable where it produces an equally robust and proportionate outcome. Some of our comments apply earlier GBBC positions on cumulative prudential requirements (CP25/15), stablecoin reserve and liquidity design (CP25/14), and international group processes (CP25/25 Part II and DP25/1).

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

The proposed guidance provides a useful account of the process and appropriately recognises that the assessment should be proportionate to the firm's activities. The remaining gap is the evidential bridge between an identified risk and the resulting own funds threshold requirement or liquid assets threshold requirement.

A clear risk-to-requirement reconciliation

PS26/12 confirms that the assessment should not duplicate requirements or operate as an additional capital layer. Without a reconciliation, the same risk event may be reflected across a K-factor, valuation haircut, cashflow stress and wind-down estimate without showing whether those measures address distinct own-funds and liquidity effects or duplicate the same quantified effect; alternatively, a resource figure may lack a clear rationale. Both make the assessment harder for management to use and supervisors to review. A short schedule should show how the firm:

1. **separately calculates the own funds and liquid assets needed for ongoing operation and wind-down;**
2. **maps common assumptions and financial effects across those assessments, K-factors, haircuts, cashflow stresses and specific liquidity requirements; and**

3. **applies the threshold mechanics and records any aggregation, correlation or diversification assumptions.**

The schedule should cross-refer to COREPRU and CRYPTOPRU and identify each component as a floor, risk proxy, stress input, mitigant or management action. For each material harm, it should explain what the relevant K-factor covers, quantify the scenario's financial effect, recognise only mitigants that work under stress, and identify any residual effect. It should also distinguish scenarios that can occur together from effects that are mutually exclusive. This does not imply mechanically deducting a K-factor amount.

If a cashflow forecast uses an asset's stressed value after haircut, the haircut should not be applied again. The FCA followed the same discipline when calibrating K-SII, distinguishing residual operational risk from the risks addressed through ILAR and the backing-asset regime. One custody example and one stablecoin example would help firms apply that distinction consistently.

Group processes with a UK legal-entity conclusion

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 firm's UK 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. This would also be consistent with the FCA's direction for firms that are both CRYPTOPRU firms and MIFIDPRU investment firms: COREPRU 7.1.1R and CRYPTOPRU 7.1.2R provide that only MIFIDPRU 7 applies, avoiding a parallel assessment under COREPRU and CRYPTOPRU 7. Although those provisions address dual-regulated firms rather than group reliance, they support the same practical principle: existing processes should be reusable where they capture the relevant risks and preserve a clear UK legal-entity conclusion.

Group support can count as own funds only once provided to the UK firm in a form satisfying COREPRU 3. Prospective funding should reduce the assessed need only where it is committed, transferable, drawable in time, available during correlated stress and not counted elsewhere.

Recreating mature group processes may add divergence as well as cost, without improving the prudential outcome. Equally, unqualified reliance could obscure resources or dependencies unavailable to the UK entity in stress. Controlled reuse, with UK governing-body ownership, provides a more credible balance. Resource allocations should follow actual wind-down actions, not revenue proxies, and exclude offsets or diversification unavailable at entity level.

The depth of modelling and documentation should likewise be proportionate. Simpler methods should be available where risk drivers and potential harm are limited; a small firm controlling substantial client assets may still require detailed analysis. Activity, client-asset control, interconnectedness, balance-sheet exposure and substitutability are more useful indicators than size alone.

Custody controls and the loss pathway

The examples do not yet show how different custody control models affect financial exposure. An example should distinguish temporary loss of access, permanent asset loss, redress liability and remediation cost, then show how MPC or multisignature controls, hardware-security modules, insurance and sub-custody affect probability, timing and recoverability where their effectiveness under stress is evidenced. This is not an argument for reopening K-RCS or assuming that delegated custody is lower risk. It is a way to ensure that the assessment follows the actual loss pathway and isolates effects not already captured by the K-factor.

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

The examples provide a helpful starting point. Their value would increase if they demonstrated the calculation and decision path, supporting consistent implementation across business models without turning non-Handbook guidance into a prescriptive template.

A stablecoin example based on legal availability

The example in paragraphs 4.14 and 4.15 is labelled for a qualifying stablecoin issuer, but currently reads as a generic encumbrance table. Read with CRYPTOPRU 7.4.6G, it should show the backing pool, assets held for token holders or safeguarded, assets available for the issuer's own obligations, and the liquidity assigned to each requirement. Accounting unencumbrance does not establish legal or operational availability.

The revised example should distinguish:

4. **backing assets and the legal or safeguarding basis on which they are held;**
5. **issuer-owned cash and assets allocated to the LATR;**
6. **contingent funding and other restrictions on availability; and**
7. **currency, location and time to monetise or transfer, including outside normal market hours.**

The example could test a Friday-evening redemption surge while cryptoasset markets remain open but a sterling payment, banking or repo settlement channel is inaccessible. An issuer may appear liquid on its balance sheet while some assets are not available when needed. The example should show which risk and cashflow each element of the liquid assets threshold requirement covers before determining the higher of Assessment A and Assessment B under CRYPTOPRU 7.4.5G and 7.4.6G, and should demonstrate that the firm holds the total sum required without double-counting the same liquid asset.

Show one end-to-end stress and wind-down example

A single worked example should trace the event, loss and cashflow profile, baseline requirements, mitigants, Stage 2 need, recovery triggers and the point at which wind-down must begin. It should distinguish out-of-hours and 24-to-48-hour liquidity, the remainder of the 90-day forecast and resources through exit. It should also reconcile paragraph 2.15's recovery after a threshold breach with paragraph 2.12's requirement to preserve wind-down resources.

For a custodian, this includes continued key-management capability, signatory retention, network fees, reconciliation and return of client assets. For a stablecoin issuer, it includes redemption outflows, out-of-hours access to reserve and payment rails, reserve monetisation and separation of backing assets from corporate wind-down resources. These steps determine the duration and cashflow of a credible exit; they are not automatically separate risks requiring additional capital.

Where representative history is unavailable, firms should be able to use relevant proxy, group or third-party data supported by expert judgement. Under paragraph 2.8, historical metrics should be selected over an appropriate timeframe and by reference to risks relevant to the firm, rather than applied as an automatic floor irrespective of the firm's exposure. Any departure should be evidenced. Controls should alter transmission or loss only where they remain effective under stress, not reduce the external shock itself.

Finally, the FCA should complete the sentence in paragraph 2.8, replace "creditors" defaulting with "debtors or counterparties", as appropriate, and review paragraph 4.1's apparent treatment of creditors as a source of cash.

Taken together, these additions would not make the guidance more prescriptive. They would make the FCA's intended outcomes easier to apply, evidence and supervise, while leaving room for firms to reflect their own activities, controls and potential for harm. GBBC appreciates the FCA's continued engagement with industry as the new regime moves towards implementation. We stand ready to support further discussion and, where useful, to help develop practical examples reflecting the range of cryptoasset business models in scope.