



MiCA Review 2026 | GBBC Response

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).



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 1. Should crypto-assets that qualify as financial instruments as defined in Directive 2014/65/EU of the European Parliament and of the Council, continue to be governed by sectorial legislation (MiFID/MiFIR/MAR/Prospectus Regulation, etc.), or should all assets that are recorded and transacted on distributed ledgers and that meet the definition of a crypto-asset, or the services provided on such assets, in principle be covered by MiCA?

Crypto-assets that qualify as financial instruments should remain governed by the main sectoral legislation. The boundary is not yet sufficiently predictable in difficult cases, but that is a reason to improve classification and supervisory convergence, not to move DLT financial instruments into MiCA.

The governing principle should be technology neutrality: the rights, obligations and economic exposure created by an instrument determine its classification. Recording or transferring the instrument on DLT should not displace MiFID II, MiFIR, MAR, the Prospectus Regulation, the CSDR framework or the DLT Pilot Regime where those rules regulate the same product and activity. Bringing DLT financial instruments into MiCA would create a parallel product regime, weaken comparability with off-chain instruments and invite regulatory choice based on technical form.

MiCA should therefore remain a regime for crypto-assets that are not already regulated as financial instruments or another sectoral product. The Level 1 text should also make clear that the exclusion follows the instrument through its lifecycle. A tokenised bond should not become a MiCA asset when it is held, transferred or traded through a crypto-native interface; equally, a service should not escape the relevant sectoral requirements because part of its technical execution is performed by a smart contract.

GBBC recommends that the Commission and ESAs implement four changes:

- **Confirm in Level 1 that classification follows the legal and economic substance of the rights, and that DLT is not an independent reason to apply MiCA.**
- **Separate asset classification from service classification. The applicable service regime should be identified by the function performed - issuance, brokerage, custody, operation of a trading venue, settlement or transfer - and duplicative authorisation should be removed where one regime already addresses the risk. The service regime should attach to the person with the capacity to perform the regulated function. The Commission and ESMA should clarify that providing software, infrastructure or part of a signing process to a client or regulated entity, without independent authority to dispose of client assets and without otherwise performing a regulated service, should not by itself require CASP authorisation. The assessment should consider the contractual role and practical control across the whole arrangement, including coordinated control, rather than infer custody from hosting infrastructure or holding a key fragment alone.**



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

- **Use the existing ESA-led convergence framework under MiCA Article 97 for novel or disputed classifications, with the relevant ESA coordinating across sectoral regimes and national authorities supplying the case evidence. Before creating another procedure, identify where the existing opinion process fails to resolve a material disagreement. Any power to make an individual determination binding across Member States would require an express additional Level 1 basis, with review and appeal rights.**
- **Address residual divergence in national implementation of MiFID II alongside MiCA convergence work. MiFID II is a directive, while MiCA is directly applicable. Guidance under MiCA cannot override differences in national law. The Commission should identify which inconsistencies can be resolved through existing supervisory powers and which require targeted legislative harmonisation of the relevant perimeter concepts.**

MiCA Article 97 already provides for ESA coordination, classification opinions requested by national authorities and reporting on divergent approaches. The joint ESA Guidelines also supply a standardised classification test and templates for explanations and legal opinions. GBBC recommends building on those mechanisms through accessible referral arrangements, reuse of existing submissions and publication of anonymised reasoning for recurring difficult cases. Any additional binding determination power should be considered only against evidenced gaps in the existing framework, rather than duplicating work already undertaken by the ESAs. ([MiCA Article 97; joint ESA final report on Article 97 Guidelines, 10 December 2024.](#))

Question 2. To what extent have ESMA's MiCA Article 2(5) guidelines and the joint ESA standardised classification test reduced uncertainty in practice? Which borderline cases remain difficult? Please explain your response and suggest any policy actions for clarification if needed.

The ESMA Guidelines and the joint ESA test are useful convergence tools. Their practical effect should be assessed through anonymised evidence of inconsistent outcomes on materially comparable facts, time taken to resolve referrals, repeat information requests and cases remaining unresolved after ESA involvement. The assessment should distinguish genuine differences in rights or applicable national law from divergent supervisory interpretation. GBBC does not infer that the existing tools have failed merely because difficult hybrid cases remain.

The most difficult cases are likely to remain hybrid governance and profit-sharing tokens; tokenised fund or money-market interests; wrapped or synthetic representations of an underlying financial instrument; commodity-referenced structures with redemption or return features; NFTs issued in a series or fractionalised after issuance; and tokens whose governance, cash-flow or redemption rights are modified after launch. Classification is also complicated where the token itself is not a financial instrument but the arrangement through which it is offered creates a derivative, collective investment undertaking or managed investment exposure.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

The Commission should resist a single-label approach. The assessment should identify the legal rights embodied in the token, the rights created by surrounding contracts and the regulated functions performed by intermediaries. A wrapper should not change the classification of an underlying financial instrument, but neither should every token referencing a regulated asset automatically inherit that classification where the holder has no corresponding legal or economic claim.

Building on Article 97 and the existing joint ESA classification test and templates, the ESAs should address the following implementation gaps:

- **extend maintained worked examples to the borderline cases identified above and publish anonymised reasons from classification opinions where confidentiality permits, showing which facts or national-law differences explain the outcome;**
- **reuse the existing explanation and legal-opinion templates and clarify how a firm can bring an unresolved case to its national authority for referral to the relevant ESA, with clear responsibility and progress reporting rather than a duplicate submission pack;**
- **issue examples covering changes after issuance and specify when a material change requires reassessment, updated disclosure or migration to a different regulatory regime; and**
- **use the existing Article 97 coordination and reporting mechanisms to identify inconsistent outcomes and explain how they will be addressed. Where a divergence cannot be resolved within current powers, identify the precise legal gap and the targeted Level 1 change required, as proposed in Question 1.**

Question 7. Which specific categories remain most difficult to classify in practice? (e.g. hybrid tokens, wrapped assets, tokenised fund interests, tokenised money-market instruments, governance tokens, synthetic exposures, or assets marketed as NFTs but issued in series)?

The most difficult cases are those in which the token, the underlying right and the surrounding arrangement point to different classifications. Priority cases for further EU guidance are hybrid governance and profit-sharing tokens; wrapped or synthetic representations; tokenised fund and money-market interests; commodity-referenced structures with redemption or return features; series or fractionalised NFTs; and tokens whose rights change after issuance.

The analysis should not stop at the label or technical wrapper. Authorities should determine whether the holder has a direct legal claim on an underlying asset, a contractual claim against an intermediary, participation in a managed pool, a derivative exposure, or only access or governance functionality. The same facts should then be tested under MiCA, MiFID II, collective-investment, banking and payment legislation in a coordinated process. Disclosure should distinguish ownership of a security from a contractual or synthetic exposure to its performance. Where voting, income or insolvency rights differ from those of the referenced instrument, those differences should be prominent; familiar asset names should not imply rights the token does not confer.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

The ESAs should publish worked examples for these categories and identify the facts that change the result. Guidance should also specify when an amendment to governance, cash-flow, redemption or transfer rights requires reassessment. This would turn the classification framework into an operational decision tool without replacing the technology-neutral perimeter recommended in response to Questions 1 and 2.

Part 2 - ARTs, EMTs and global stablecoins

Question 11.1 To what extent do you think the calculation methods are relevant?

Question 11.2 To what extent do you think the calculation methods are appropriately calibrated?

The calculation methods are relevant as prudential anchors, but they are not equally well calibrated. The current 'highest of' approach provides a useful floor; its reserve-based limb is too blunt where it treats balance-sheet size as a proxy for all material risks and does not show how reserve, liquidity and capital requirements should interact.

- **The EUR 350,000 minimum should remain as an entry floor and be reviewed periodically for inflation and operational complexity. It should not be treated as sufficient for a large or operationally complex programme.**
- **The fixed-overheads limb remains useful for orderly wind-down and operational continuity, but new and fast-growing issuers need a forward-looking calculation where preceding-year costs are not representative.**
- **The reserve-based limb should be made risk-sensitive. A fully segregated, highly liquid and conservatively managed reserve should not attract the same capital outcome as a reserve exposed to duration, credit, concentration, currency, custody or operational risk. Capital should cover loss-absorbing risks; reserve and liquidity rules should cover redemption. The same risk should not be charged twice without explanation.**
- **Additional own funds for significant tokens are justified, but threshold effects should be softened through moving averages and a phased transition. Critical liquidity, governance and reporting measures can be accelerated where risk increases, while systems-intensive changes should follow a supervised implementation plan.**

A more durable framework would retain the statutory floor and empower supervisors to apply a transparent risk add-on using common factors: reserve credit and duration risk, redemption volatility, concentration in custodians and settlement banks, operational dependencies, cross-border rebalancing exposure and the effectiveness of recovery arrangements. The methodology should be published at Union level and applied consistently, with reasons given for material supervisory add-ons. The assessment should also consider dependence on a token for settlement or margin payments, including peak obligations and the availability of substitutes. A relatively small



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

token can create concentrated operational dependencies. Any additional requirement should follow evidence of that exposure and the issuer's obligations, rather than assume that every wholesale use requires the same capital uplift.

For a multi-issuance token, capital should follow the risk borne by the EU entity - including redemption obligations, inter-issuer exposures and guarantees - rather than the historical location in which a particular unit was minted. Group-level support should be recognised only where it is legally enforceable and available within the period in which redemption must be funded, including in stress. Expected reimbursement should not reduce the reserve or liquidity needed to meet the EU entity's gross legal obligations before reimbursement arrives.

Question 12. After being in effect for close to two years, no ARTs have been licensed in the EU under MiCA. In your view, does this absence primarily reflect low market interest in ARTs or other reasons?

The absence of authorised ARTs should not be treated as a reliable proxy for low market interest. It is at least as important to examine whether viable use cases are being prevented from reaching the authorisation stage by perimeter uncertainty, a prudential model designed around payment-like stablecoins and the cost of resolving supervisory questions before product-market fit can be tested.

ARTs cover materially different structures: tokens referencing commodities, baskets, indices or other rights may serve as a means of exchange, a settlement asset, a treasury instrument or an investment exposure. A single prudential template risks over-regulating low-risk or wholesale structures while still failing to identify the risks of products whose value or return depends on investment management. The boundary with MiFID is therefore not a preliminary drafting issue; it determines the appropriate disclosure, governance, distribution and prudential regime.

The Commission should ask the EBA and national authorities to publish anonymised evidence on pre-applications, withdrawn applications, material deficiencies and average decision times. This would distinguish low demand from regulatory attrition without exposing confidential files. Policy should be based on that evidence rather than the headline number of licences.

GBBC recommends a coordinated two-stage approach for novel ARTs, using existing procedures:

- **early classification assessment using the existing ESA test and legal-opinion template, with unresolved cases referred through Article 97 as described in Questions 1 and 2, before the applicant incurs the cost of a full authorisation file; and**
- **a proportionate authorisation pathway calibrated to the stabilisation mechanism, redemption commitment, reserve composition, distribution model, holder type and scale of use.**

This is not a case for weakening core safeguards. Reserve segregation, reliable valuation, clear holder rights, custody and recovery planning should remain. The objective is to apply those safeguards to the risk the product actually creates rather than to the ART label alone.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 13. If ARTs were to come to market, what do you think is the primary purpose from a consumer/investor perspective: investment or alternative means of exchange/payment? Please explain your answer:

The question presents investment and exchange or payment as alternatives, but the ART category is broad enough to contain both. The primary purpose should be established from the rights, stabilisation mechanism, distribution strategy and actual use of the particular token rather than assigned to ARTs as a class.

An ART designed for settlement or treasury use may function predominantly as a means of exchange. A commodity-, basket- or index-referenced token may instead be acquired primarily for economic exposure or capital appreciation. Programmability can also allow the same token to support settlement in one context and investment in another. A single answer would obscure these differences and could produce the wrong disclosure, distribution and prudential treatment.

The Commission should adopt a functional use-case assessment and require the white paper to identify the intended primary use, material secondary uses and the features supporting that assessment. Where investment characteristics are material, authorities should complete the MiCA/MiFID and collective-investment perimeter analysis before authorisation. Where payment use is material, reserve liquidity, redemption access, operational resilience and the interaction with payment-services law should receive greater weight.

Question 14. MiCA requires issuers of ARTs to establish, maintain, and prudently manage a reserve of assets and appropriate liquidity arrangements to ensure orderly redemptions and mitigate financial stability, liquidity, and operational risks. Additional and enhanced requirements apply to ARTs classified as “significant” under Article 45. How do you think, if at all, each of the following elements of the MiCA liquidity and reserve regime for ARTs should be adjusted?

The obligation to maintain a segregated reserve capable of supporting redemption should remain. The adjustment should be in calibration: fixed asset-allocation rules should give way to an outcomes-based liquidity standard that is demonstrably capable of meeting normal and stressed redemptions without forced sales or dependence on discretionary group support.

The 30% and 60% minimum deposit requirements should be reviewed alongside the concentration and counterparty risks they may create. Deposits are not risk-free, and a mandatory allocation can concentrate exposure to a limited banking network. The rules should permit an appropriate mix of immediately available deposits and high-quality liquid assets, subject to conservative haircuts, maturity limits, currency matching, diversification and tested same-day monetisation. Supervisors should be able to require more cash where the redemption profile warrants it, but the percentage should not operate as a universal proxy for liquidity.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Commodity-referenced and other non-currency ARTs require a distinction between economic backing and redemption liquidity. The assets that preserve reference value may not be the assets best suited to fund immediate redemption. A compliant structure should therefore be able to maintain a legally isolated reference-asset or hedging pool together with a separate liquidity sleeve, provided valuation, margining, top-up and liquidation rules are transparent and enforceable. Trustee or independent control over specified stress triggers can strengthen this model.

Audit and custody requirements should remain robust but become more interoperable. One reserve should not require duplicative audits for each co-issuer if a group-wide audit, local attestation and regulator access produce the same assurance. Custody diversification should be driven by exposure and substitutability, while legal opinions should confirm segregation, priority and enforceability in every relevant jurisdiction.

For significant ARTs, enhanced stress testing and reporting are appropriate. The stress framework should include rapid cross-border migration of tokens, weekend or bank-holiday redemptions, failure of a custodian or settlement bank, delayed reserve transfers, currency dislocation and the loss of a co-issuer. Results should determine firm-specific liquidity and recovery actions rather than automatically producing a fixed EU ring-fence.

Question 15. MiCA sets out liquidity and reserve requirements for issuers of EMTs to ensure immediate redemption of tokens, mitigation of credit and operational risk, and resilience under stress scenarios. Additional requirements apply to EMTs classified as “significant” (Article 56). Should any of the following aspects of the MiCA regime for EMTs issued by e-money institutions be adjusted?

The core EMT safeguards should remain: full backing, legal and operational segregation, immediate redemption, independent assurance and enhanced liquidity management for significant tokens. The principal adjustment should concern how liquidity and concentration are calibrated, not whether the reserve exists.

GBBC would retain the reserve, segregation, audit and custody requirements broadly unchanged, subject to technical simplification where equivalent assurance is available. Enhanced stress testing and high-frequency monitoring for significant EMTs should be strengthened where the token has material payment, settlement or cross-border use. Stress tests should demonstrate how reserves become usable redemption liquidity within the relevant payment and settlement windows, including outside banking hours and during a custodian or settlement-bank outage. This requires evidence of access rights, conversion times and contingency arrangements. Equivalent safeguards should be recognised across eligible providers; a prescribed custody allocation or preferential claim for a settlement intermediary should not weaken protection for other token holders.

The fixed 30% and 60% deposit shares should be recalibrated. A common minimum liquidity floor remains appropriate, but the eligible mix should reflect currency matching, same-day monetisation, maturity, credit quality, diversification and the issuer's observed redemption profile. Requiring



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

deposits beyond the level needed for operational liquidity can concentrate exposure to a small banking network without necessarily increasing the reserve's resilience.

The 1.5% bank/token concentration limit is a useful backstop against excessive interconnectedness, but it should be reviewed as part of the same framework. Any alternative method should preserve a binding concentration control, use consistent definitions of exposure and allow supervisors to impose a lower limit where the issuer or deposit-taking counterparty is systemically important. The final calibration should be supported by impact analysis covering both bank and non-bank EMT issuers.

Question 20. In your view, should the MiCA prohibition on granting interest or any interest-equivalent remuneration be modified?

GBBC supports assessing a narrowly defined form of variable remuneration, rather than recommending unconditional removal of the prohibition. The assessment should preserve the distinction between EMTs and deposits and address financial stability, deposit substitution and redemption incentives before any legislative change is proposed.

The Commission should examine whether the prohibition displaces activity towards less transparent arrangements or non-EU platforms, alongside any benefits in limiting deposit substitution and additional reserve risk. Evidence should cover actual customer behaviour, the source of remuneration and the consequences for bank funding and stablecoin redemptions. Those effects should be tested rather than assumed.

The assessment should be limited to a model with the following safeguards:

- **no payment from reserve principal or regulatory capital, with required reserve backing, own funds and liquidity preserved;**
- **variable remuneration with no promised yield, supported by clear disclosure of its source, deductions and the absence of deposit-guarantee protection;**
- **no impairment of immediate redemption, including EMT redemption at par and the applicable ART redemption right, and no holding-period condition that restricts that right;**
- **no maturity transformation, additional leverage or expansion of the permitted reserve risk profile to fund remuneration; and**
- **a workable means to reduce or stop prospective remuneration as available income changes, without reducing reserve principal or restricting redemption. The Commission should test the safeguards under stressed conditions as well as in normal markets.**

The assessment should distinguish professional clients and eligible counterparties, as defined under MiFID II, from retail holders. It should examine whether any different treatment is justified by the risks and protections involved. A possible retail model could be limited to variable pass-through of



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

realised net reserve income, subject to the safeguards above; this is an option for assessment, not a recommendation for immediate permission.

The Level 1 text should also separate issuer-paid remuneration from independent services such as staking, lending, rebates or loyalty programmes. Those activities should be regulated according to their own economic function and risk. A CASP should not be able to circumvent issuer rules, but neither should every benefit offered by a third party be treated automatically as interest on the token.

Any legislative proposal should follow that assessment and resolve whether the remuneration arrangement changes the product's classification under MiFID II, collective-investment or banking rules. Permission under MiCA should not override those regimes. Relabelling interest as a reward or return should not circumvent the current prohibition.

Question 29. Based on your experience and assessment, how significant are the following risks associated with a multi-issuance model of global stablecoins for the EU financial system?

The risks are material but strongly design-dependent. The most significant risks arise where the EU issuer must redeem fungible tokens without a legally enforceable right to obtain corresponding liquidity or reimbursement from other issuers, and where supervisors cannot observe or constrain that exposure in time. Multi-issuance should not be treated as risky merely because several legal entities mint the same token; the relevant question is how liabilities, reserves, information and losses move across the network. The analysis in [The Multi-Issuance Issue](#) (Bindseil, Georg, Hansen and Melches, 7 September 2026) reinforces the need to test how arbitrage can redirect redemption pressure towards the accessible issuer. It also argues for assessing direct EU distribution of well-regulated foreign stablecoins under an equivalence regime. GBBC considers that alternative worth evaluating against the enforceability and liquidity safeguards below; reserve location alone should not be treated as proof of protection.

Arrangements involving only MiCA-authorised EU issuers should be distinguished from those involving a third-country co-issuer. In the latter case, an EU authority cannot assume that its directions will bind the foreign issuer or its supervisor. A contractual reimbursement claim may also be too slow to provide liquidity during a run. The assessment must establish what resources remain accessible if the foreign issuer defaults or its jurisdiction restricts transfers. Recognition should therefore operate at two levels: an assessment of the relevant third-country regime and a separate decision on the individual issuer or arrangement. A positive jurisdiction-level assessment should not automatically confer market access on every issuer established there.

Minting origin is not a stable measure of risk. A token can move between jurisdictions and wallets immediately, while redemption may occur through a different issuer. Prudential assessment should distinguish the EU entity's gross legal redemption obligations, the liquidity required before reimbursement and its net economic exposure under normal and stressed conditions, informed by EU distribution and holding data, redemption patterns, inter-issuer balances and plausible inflows



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

during stress. Unknown self-hosted holdings should be addressed through conservative estimates and tolerance bands, not an assumption that every unclassified token is an EU liability.

The risks should be addressed through minimum operating conditions:

- **a uniform minimum redemption right for holders of the fungible token, with clear identification of the entity against which the claim can be exercised;**
- **legally enforceable inter-issuer settlement and reimbursement arrangements, backed where necessary by accessible collateral or prefunding contributed by the co-issuer creating the exposure, and a default waterfall if an issuer fails;**
- **daily or risk-triggered exposure reporting, common data standards and regulator access to group-level reserve and circulation information;**
- **home-host cooperation covering recovery, resolution, reserve transfer restrictions, emergency powers and communications; and**
- **targeted safeguards for gaps in enforceability, transferability or home-jurisdiction standards, with their cost and funding allocated across participating issuers according to the risks they create;**

These safeguards target the mechanisms that produce run and contagion risk. A requirement to fragment the token or hold a fixed reserve solely by minting origin could reduce fungibility and trap liquidity without ensuring that it is available where redemption occurs.

The framework should preserve commercially viable EU participation while maintaining effective holder protection. Supervisors should give reasons for additional local requirements and assess their combined effect with overseas reserves, capital and support obligations. The absence of direct EU powers over a foreign co-issuer should not, by itself, make the EU entity the guarantor of the entire global arrangement.

Question 30. MiCA does not currently prohibit multi-issuer models, nor does the EU have jurisdiction to determine how third country entities, that also have licensed entities in the EU, should be regulated in third country jurisdictions. Given your assessment of the advantages or disadvantages of global stablecoins and multi-issuance models, do you think that MiCA should continue to be open to multi-issuance models?

Yes. MiCA should remain open to multi-issuance and should state the conditions for it at Level 1. Legal uncertainty is not an effective risk control: it discourages compliant EU participation while global tokens remain accessible through other channels.

Multi-issuance can support globally fungible liquidity, cross-border payments and settlement of tokenised assets while keeping an accountable regulated entity in the EU. It can also diversify operational capacity. Those benefits depend on a design in which the EU issuer is not a thin



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

distribution vehicle and EU holders do not depend on discretionary support from a third-country affiliate.

Level 1 should require:

- **an authorised EU co-issuer responsible for its issuer-side MiCA duties, with a clear allocation of redemption obligations, reserve governance, disclosures, recovery planning and regulatory reporting. This should not create an automatic guarantee by that entity of every foreign co-issuer obligation;**
- **a documented allocation of liabilities and reserve assets, with liquidity available to meet obligations as they fall due and enforceable, tested settlement arrangements between issuers;**
- **common minimum holder rights across fungible units, so that technical interchangeability is not paired with hidden differences in legal protection;**
- **group-wide governance, data and stress testing, with an EU recovery playbook and clear consequences if a third-country issuer or transfer channel becomes unavailable; and**
- **proportionate information-sharing and cooperation arrangements with relevant third-country authorities, supported by enforceable obligations on participating issuers. Formal equivalence should be an additional route to reducing duplication, rather than a prerequisite for every multi-issuance model.**

CASPs should not be made responsible for issuer functions they cannot perform. They can identify customers, apply distribution and conduct rules, supply relevant transaction data and operate redemption access points. They cannot create reserve assets, compel a co-issuer to rebalance or absorb an issuer's insolvency risk. Assigning those duties to CASPs would obscure rather than strengthen accountability.

Question 34. MiCA provides safeguards to mitigate the risks of multi-issuance stablecoins. For each safeguard listed below, please indicate how effective you consider it to be:

The safeguards are relevant, but they do not all address the specific failure channels created by multi-issuance. Reserve, liquidity, EU establishment and intervention powers are important foundations. None substitutes for enforceable allocation of redemption liabilities, inter-issuer settlement, group-level information and an operational mechanism for moving liquidity under stress.

For the online ratings, GBBC's qualitative assessment is:

- **Reserve location, composition and liquidity requirements: potentially highly effective, provided they follow actual redemption exposure and are supported by enforceable access to liquidity rather than minting origin alone.**



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

- **EU establishment and the ECB, EBA and competent-authority intervention powers: moderately to highly effective as accountability and crisis tools, but dependent on timely information and a clearly identified EU issuer with the capacity to act.**
- **Restrictions linked to use of a non-EU currency: only moderately effective and potentially blunt. They may limit scale but do not resolve fungibility, reserve transfer or legal-enforceability risks in the remaining market.**
- **National intervention powers: necessary, but less effective where uncoordinated use fragments a cross-border arrangement or conflicts with actions taken by the EBA, the ECB or a third-country supervisor.**

The review should therefore preserve these safeguards but connect them through a Union-level multi-issuance framework specifying the EU supervisory anchor, common data, rebalancing, recovery and default arrangements. Effectiveness should be tested through joint supervisory exercises, including failure of a third-country co-issuer or a prohibition on transferring its reserves. EU establishment and intervention powers do not themselves compel a foreign entity to supply liquidity.

Question 35. MiCA requires that the reserves of the EMTs and ARTs issued, offered or held in the EU should be held in the EU. Can the tokens held in the EU be determined or estimated with sufficient accuracy and frequency?

Only partially. Public ledgers can show addresses and movements, but they do not ordinarily reveal the residence of the beneficial holder or the jurisdiction in which redemption pressure will arise. CASP data improves the picture for hosted holdings, while self-hosted wallets, omnibus arrangements, bridges and rapid cross-border transfers prevent exact and continuous attribution.

MiCA should not impose a compliance test that requires an issuer to know information that the technical system does not contain. Nor should minting origin be used as a substitute: it identifies an operational event, not the current holder or the entity likely to face redemption. A requirement based on false precision would encourage inconsistent models and potentially excessive reserve localisation.

The EBA should specify a supervisor-approved EU-exposure methodology combining: holdings and flows attributable to EU-authorised CASPs; issuer and distributor customer data; direct redemption data; inter-issuer balances; and statistically reasonable estimates for self-hosted wallets and unidentified flows. The methodology should use defined confidence levels, reconciliation frequencies and conservative buffers that reflect uncertainty and volatility. Its cost should be assessed against the improvement in risk measurement, and net estimates must not displace the gross-obligation and reimbursement-timing assessment described in Question 29. Common data definitions, identifiers and reporting interfaces should allow CASPs, custodians and issuers to reuse validated information. Reconciliation should distinguish tokens in circulation from reserve assets and record valuation times and encumbrances. Supervisory reporting should replace a duplicate



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

issuer request only where the issuer can lawfully obtain the information in time to meet its own obligations, with confidentiality and data protection preserved.

Compliance should be assessed against tolerance bands and governance standards, not point estimates. Documented use of an approved methodology should constitute rebuttable evidence of reasonable compliance efforts where later information changes an estimate. It should not excuse failure to update the estimate, respond to warning signs or meet applicable reserve obligations. Supervisors should retain power to require a higher buffer where data quality is persistently weak or stress inflows are plausible.

Self-hosted wallets should remain part of the exposure estimate, but users should not be required to surrender wallet autonomy or disclose identity merely to make the reserve calculation administratively easier. The regulatory objective is adequate EU liquidity and enforceable redemption, not comprehensive geolocation of every token.

Question 36. Should MiCA redemption rights be explicitly limited to EU holders only?

No. Limiting the legal redemption right by holder location is difficult to reconcile with a fungible bearer-like token, creates uncertainty at the point of stress and may discriminate against users of self-hosted wallets who cannot demonstrate location through an EU intermediary.

The location of a holder can change faster than an issuer can update reserve allocation, and legal residence, physical location, wallet provider and place of acquisition may all point to different jurisdictions. A location-based right would therefore require an arbitrary connecting factor and could create two economically identical units with different legal value. That fragmentation may itself increase run incentives.

EU protection should instead attach through issuer authorisation, offering and distribution rules, an accountable EU redemption channel and reserve calibration based on EU exposure. Concerns about tokens moving into the EU during stress should be addressed at issuer level through liquidity buffers, inter-issuer settlement and recovery triggers. They should not be addressed by removing the redemption right from a class of holders at the moment when confidence is most fragile.

A common minimum redemption right does not require every holder to have an unlimited claim against every co-issuer. Legislation should distinguish the holder's claim, the legal debtor and any redemption agent, and assess four models: (i) several liability, with each issuer responsible for an identifiable allocation and an enforceable way to identify the debtor after transfers; (ii) joint redemption access backed by mandatory inter-issuer reimbursement, collateral and liquidity available before reimbursement arrives; (iii) an EU redemption agent acting for a legally responsible foreign issuer, with enforceable recourse and appropriate recognition and supervision; or (iv) an issuer-of-record model with internal group settlement. Each model must preserve existing statutory claims and explain how fungible units receive the same transparent minimum protection. If debtor allocation cannot remain reliable after transfers, the several-liability model should not be



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

used for an undifferentiated fungible token. The EU entity should fund its actual legal obligations, including gross redemptions pending reimbursement, without automatically guaranteeing the full global supply. The foreign-issuer model would require the express legislative route discussed in Question 41.

Redemption remains subject to applicable sanctions, anti-money laundering and customer due-diligence requirements. Those controls are distinct from a general rule that only EU holders possess a claim.

Question 37. In a multi-issuance model, reserve assets may be located across jurisdictions and legal entities. Concerns have been expressed that in times of market stress, the transfer or rebalancing of reserves between issuers may be delayed or restricted. Is this concern valid or substantiated in your view?

The concern is valid in principle, but it is not inherent in every multi-issuance model. Its severity depends on where assets are held, the legal form of inter-issuer claims, settlement and banking arrangements, capital or exchange controls, insolvency law and the powers available to home and host supervisors.

MiCA should require an ex ante rebalancing policy approved by the relevant supervisors. It should specify the exposure measure, quantitative and qualitative triggers, decision rights, maximum execution times, eligible transfer channels, required collateral or prefunding, priority of claims and the allocation of losses or liquidity shortfalls. It should cover weekends, bank holidays, failure of a settlement bank, cyber or operational interruption and a direction by a third-country authority that prevents transfer.

The legal agreement between co-issuers should be enforceable independently of ordinary group discretion. It should create a clear reimbursement claim, provide information and audit rights, define default and dispute procedures and link a failure to rebalance to recovery actions. Legal opinions should address insolvency, transfer restrictions and access to collateral in the relevant jurisdictions. Liquidity credit should be given only to resources that can be accessed within the required redemption timetable. Co-issuers creating the exposure should contribute the necessary prefunding or collateral. Supervisors should test the mechanism under non-performance, rather than relying only on contractual representations.

A fixed EU ring-fence should be a residual measure where enforceability or cooperation is inadequate, not the default model. Ring-fencing can increase local resilience, but it can also fragment a common liquidity pool and make rebalancing harder. A proportionate regime should permit equivalent outcomes through prefunding, committed liquidity, collateralised inter-issuer exposures or sufficiently reliable transfer arrangements.

The Commission should establish minimum requirements for supervisory information-sharing, stress coordination and crisis communication. Those arrangements cannot guarantee that a third-



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

country authority will permit a transfer in stress. Where cooperation is limited, accessible prefunding or collateral may address the resulting gap. If timely redemption cannot be protected, the arrangement should be changed or not approved, with any restriction on an existing arrangement preserving accrued holder claims and providing for orderly redemption. Full mutual recognition should not be a precondition where effective, proportionate safeguards can be demonstrated.

Question 38. How effective would the following possible additional measures be in mitigating such concerns?

The most effective measures are those that increase available liquidity, information and enforceability before stress occurs. Measures that divide redemption rights by wallet type, client relationship or holder status are less effective and may create new incentives to run.

- **A dedicated EU liquidity buffer calibrated to stressed redemption outflows falling due before reimbursement, taking account only of resources accessible within that period: highly effective where required by data quality, transfer constraints and enforceability; it should not become a fixed duplicate reserve unrelated to risk.**
- **High-frequency reserve and liquidity reporting, including location and transfer constraints: highly effective, provided the data are standardised and available to the relevant home and host authorities.**
- **Supervisory cooperation and tested cross-border transfer procedures: effective where supported by relevant legal powers and enforceable issuer commitments. Cooperation cannot override foreign insolvency law or transfer restrictions; accessible resources must cover the period in which transfers are unavailable.**
- **Enhanced rights for tokens shown to circulate genuinely in the EU: limited effectiveness because holder location and circulation can change rapidly and are difficult to establish for self-hosted holdings.**
- **Restricting redemption to clients of EU-authorised CASPs: ineffective and disproportionate. It would penalise lawful self-custody and make an intermediary relationship determine the value of an otherwise fungible unit. The issuer should identify and verify the redemption claimant through its own onboarding and applicable customer due-diligence procedures, whichever wallet the token arrives from. A separate CASP relationship should not be a condition of redemption where the issuer can obtain the necessary verification directly; requiring that relationship adds no necessary verification safeguard in those circumstances.**
- **Differentiating legal redemption rights between retail and professional holders in crisis: generally ineffective. Operational channels and disclosure may differ, but ex post alteration of claim priority would increase uncertainty unless established transparently as part of the instrument from issuance.**



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 39. If you referred in your response to question 38 to adjusting redemption rights, please provide any comments on the operational feasibility, legal implications, proportionality, or potential intended or unintended consequences of such amendments the redemption rights in MiCA as listed above or in any other way:

GBBC does not recommend making the existence or priority of the core redemption claim depend on the holder's location, use of an EU-authorised CASP or retail/professional status. Those criteria can change during the life of a fungible token, may not be observable in self-hosted wallets and could cause identical units to carry different legal value precisely when certainty is most important.

A location-based preference could also encourage migration into qualifying accounts as stress develops, accelerate redemptions and require issuers to make contested eligibility decisions under severe time pressure. Restricting self-hosted holders would weaken technological neutrality and could turn custody choice into a condition of substantive property or contractual rights.

MiCA should instead preserve a common minimum redemption claim, identify its legal debtor or debtors as described in Question 36, and manage exposure through liquidity buffers, enforceable inter-issuer reimbursement, data and recovery triggers. The allocation of obligations must not make the EU co-issuer a default guarantor for all foreign issuance. If any contractual subordination or different redemption channel is permitted, it should be transparent from issuance, objectively justified, consistent with insolvency law and incapable of being changed retrospectively during stress.

Question 40. Do you see merit in introducing an equivalence regime for global stablecoins in the EU?

Please provide reasons for your response, including any perceived advantages or disadvantages of equivalence regimes.

Yes, in addition to targeted mitigation measures. It should be an optional route that allows the EU to recognise prudential and supervisory outcomes achieved abroad while retaining an accountable EU nexus for distribution, data, redemption access and residual local risks.

Without recognition, a global arrangement may be required to duplicate reserves, capital, governance and reporting even where the third-country regime produces an equivalent outcome. Duplication can fragment liquidity and discourage an EU issuer from participating in the global token. At the other extreme, automatic reliance on international standards or the existence of a foreign licence would not be sufficient because implementation, enforceability and supervisory cooperation differ.

Equivalence should be outcomes-based and assessed against published criteria: reserve quality, segregation and location; redemption rights; capital and liquidity; governance and operational resilience; disclosure; recovery and resolution; supervisory powers; access to information; and enforceability of cooperation in stress. The jurisdiction-level decision should assess the relevant



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

stablecoin regime. A separate assessment of the issuer or arrangement should determine eligibility to rely on that decision and any targeted safeguards. This avoids assuming that a regime-level finding resolves every entity-specific risk. Issuer-specific recognition should require effective ongoing supervision, access to information, enforceable redemption arrangements and the capacity to comply with targeted EU safeguards. Equivalence must not become an indirect passport for an inadequately supervised issuer.

A positive decision should be monitored, reviewable and revocable. The framework should provide advance notice, published reasons, a remediation period where appropriate and an orderly transition for existing holders, preserving redemption and the resources needed to fund it. Authorities should retain power to impose immediate restrictions where an urgent risk requires them; withdrawal should not itself extinguish existing holder claims or force disorderly liquidation. The Commission should publish the assessment timetable and information requirements. Equivalence should not depend on political reciprocity where third-country outcomes and EU safeguards are otherwise adequate, although reciprocal market access can be considered separately.

Multi-issuance should also remain possible without a completed equivalence decision where the arrangement meets the operating conditions described in Questions 29, 30 and 37. Market access should not depend on reciprocal recognition or a jurisdiction-wide decision that an issuer cannot obtain for itself. Any additional requirement should address an identified gap and recognise safeguards already provided by participating issuers. Such a route must still require an issuer-specific assessment and effective supervisory cooperation; it should not bypass the safeguards required for recognition.

Question 41. Equivalence regimes can rely on the third country's regime to various degrees. How far, in your opinion, should a possible equivalence regime go in terms of relying on third-country regime? What rights or benefits should EU issuers derive from equivalence of a third country and what rights or benefits in the EU should issuers from an equivalent jurisdiction receive in the EU?

Equivalence should permit reliance on the third-country regime for issuer-level prudential, reserve, governance, audit and group-supervision requirements where those outcomes are demonstrably comparable. EU rules should continue to govern EU offering and distribution, conduct towards EU clients, the accountable EU contact, access to redemption and any additional local liquidity required by residual risk.

Within a recognised multi-issuance arrangement, a third-country co-issuer should be able to rely on recognised audits, custody arrangements, prudential calculations and regulatory reports, subject to EU access to the underlying information. The authorised EU co-issuer proposed in Question 30 should remain accountable for its allocated MiCA obligations. A representative appointed only to receive communications cannot discharge issuer reserve or redemption duties. Any route allowing direct EU offering by a third-country issuer without an EU co-issuer would require an express



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

legislative exemption and separately specified holder protection; it should not be assumed to follow from listing by a MiCA-authorised CASP.

EU issuers operating in relation to an equivalent jurisdiction should receive corresponding recognition where that jurisdiction offers it, including recognition of EU prudential supervision and avoidance of duplicate local reserves. The EU decision cannot itself confer rights under foreign law, so the Commission should distinguish unilateral EU recognition from negotiated reciprocal arrangements.

The correct model is graduated reliance. Reliance should extend only to functions shown to achieve the required outcome in the recognised arrangement; local rules remain appropriate for EU-specific conduct and enforceability. Where a particular safeguard is not equivalent, the EU should impose a targeted top-up for that gap rather than reject the entire regime or recreate the foreign authorisation in full.

Part 3 - CASPs and payment-services overlap

Question 45. Is the list of crypto-asset services as defined in Article 3(16) of MiCA adequate to effectively cover crypto-asset markets and provide sufficient legal clarity for businesses?

The list requires clearer application to technology providers, particularly where custody and signing are split between several parties. The Commission and ESMA should distinguish the person undertaking a regulated service for a client from a provider supplying software, infrastructure or a constrained part of the signing process on that person's or the client's instructions. A provider's role in hosting systems or holding a key fragment should not, by itself, determine the need for authorisation.

As proposed in Question 1, obligations should attach to the person capable of performing the relevant function. Guidance should assess who safeguards the assets or means of access, who can authorise or execute disposal, and whether parties exercise coordinated control. It should protect the distinction for pure technology provision without allowing a custodian to avoid responsibility by dividing keys or outsourcing part of its operations. The same functional assessment should cover order and execution management systems. ESMA should distinguish supplying software from actually receiving, transmitting or executing client orders, and from operating a multilateral trading system under [MiCA Article 3](#). A software label should not conceal a regulated service, while connectivity or order-routing functionality alone should not automatically make its supplier a trading-platform operator.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 54. Given that crypto-asset service providers are entities subject to the regulatory framework of the Digital Operational Resilience Act (DORA), are there any additional issues/challenges that need to be addressed in relation to cybersecurity?

The review should address overlapping ICT outsourcing requirements and specify technology-neutral outcomes for key management. Where an arrangement falls within DORA, compliance with its requirements should discharge the corresponding MiCA Article 73 requirements for that arrangement. The Commission should provide an express recognition rule, supported by a mapping of equivalent obligations, so that one relationship does not require two sets of policies, contracts and assurance evidence. Any distinct MiCA duty should be identified and retained, including the CASP's responsibility to clients and effective supervisory access. The Commission and ESMA should also clarify how sub-custody under [MiCA Article 75\(9\)](#), outsourcing under Article 73 and ICT services under DORA interact. Worked custody-chain examples should identify the applicable duties without assuming that every sub-custody arrangement is either outsourcing or exempt from it. Recognition of equivalent controls should preserve client information, segregation, oversight and responsibility for returning assets.

Key-management requirements should specify outcomes rather than mandate a particular architecture: no single individual, external provider or component should be able to dispose of client assets alone outside independently enforced approval controls; each client's assets and entitlements should be separately identifiable and segregated; recovery should be tested; and a complete evidence trail should record signing instructions, approvals and execution. Hardware security modules (HSMs), threshold-signature and multi-signature designs should all be eligible where the complete arrangement demonstrates these outcomes. Splitting keys should not transfer the regulated custodian's responsibility to a technical participant or make recovery dependent on an unavailable provider.

Recognised third-party assurance, including independent security audits, SOC 2 Type II reports and ISO 27001 certification, should be reusable across a provider's CASP clients where it covers the relevant systems and controls. Supervisors should recognise a common evidence pack and pooled audits, with additional testing directed to uncovered risks, material changes or identified deficiencies. These forms of assurance have different scopes and should not be treated as interchangeable proof of compliance. Each CASP should assess relevance, currency and control effectiveness, retain necessary audit and access rights, and remain accountable for its third-party risk management.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 55. The Payment Services Directive has been substantially reviewed recently, bringing notably more clarity on the interplay between the MiCA rules applying to the transfer services in relation to e-money tokens and the rules under the payment services framework which apply to the provision of payment services. As a result, the PSD3/R will clarify which crypto-asset services may qualify as payment services, including targeted exclusions from the scope of PSD3/R for specific types of transactions/exchanges involving EMTs, and will specify the authorisation process under PSD3 in cases where CASPs are required to obtain a PSD3 authorisation. Do you consider these changes bring sufficient clarity or are there other issues that remain to be addressed?

Not fully. GBBC welcomes the targeted exclusions and streamlined authorisation provisions in the 17 April 2026 final compromise texts (Council documents [8221/26, PSR](#), and [8222/26, PSD3](#)). Our assessment refers to those texts and their article numbering, rather than treating their proposed changes as already applicable law. The remaining questions concern the scope of individual services, additional payment obligations and consistent implementation. Our objective remains a coherent authorisation route with additional requirements confined to payment risks not already addressed by MiCA.

The starting point is the operative exclusions in PSR Article 2, read with recital 29a. These cover specified EMT exchanges and direct payments without an intermediary; they do not exclude every transfer bundled with a MiCA service. The recital supplies context and cannot extend the exclusions. Under the EBA's PSD2 approach, own-wallet transfers can still be payment services, and wallets enabling third-party transfers may be payment accounts. Guidance should therefore identify the service and applicable exclusion, rather than infer exclusion simply because an EMT is used in a trade.

PSD3 Article 3(3a) provides for reuse and updating of specified MiCA application material. Article 13(2a) provides a 60-business-day decision period for authorised CASPs applying to provide payment services only with EMTs, subject to suspension for missing information. These provisions streamline an authorisation requirement; they do not remove it. GBBC asks that implementation maximise reuse of the existing file and confine additional requests to the payment services envisaged.

PSR Article 110b would insert MiCA Article 60(4a), allowing a payment institution to notify specified equivalent EMT services for payment purposes at least 40 working days before starting them. Its operative mapping covers custody, exchange, transfers, execution of orders, and reception and transmission of orders against specified PSD3 payment services. The Commission should explain how that mapping interacts with Article 2 exclusions and compare it with the CASP application route. Existing authorisation work should receive equivalent recognition whichever licence the firm obtained first, with remaining differences justified by the services and risks involved.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Building on these provisions, the Commission, EBA and ESMA should publish common implementation guidance and use their respective rule-making powers where a binding requirement is needed. The Commission should provide an explicit mandate for joint EBA–ESMA guidance establishing a common service taxonomy and perimeter interpretation, building on existing mandates and proposing a targeted legislative basis only where necessary. This work should:

- **map EMT issuance, custody, exchange, transfer and payment activities to the applicable regime. Worked examples should distinguish excluded trading transactions from payment services, including bundled services, merchant payments, own-wallet transfers and transfers involving self-hosted addresses. Any criteria concerning transaction purpose must remain within the statutory exclusions and should not require firms to infer customers' undisclosed intentions. Pure technology provision should not trigger authorisation solely because it supports payment execution. The mapping should preserve the technical-service exclusion while distinguishing payment initiation, account information and other independently regulated functions. Operational and outsourcing risks remain subject to applicable controls; absence of possession is not, on its own, proof that no regulated service is performed;**
- **make streamlined authorisation effective in practice. The EBA should use the mandate in PSD3 Article 3(5), which expressly covers CASP applications under Article 3(3a), to standardise information requirements and assessment methodologies and maximise reuse of MiCA documentation. A common checklist should distinguish material to be reused, updated or newly supplied, identify the responsible authority and coordinate requests where supervisors differ. Authorities should explain repeat requests and publish comparable processing-time data;**
- **assess how payment orders, execution, identifiers, refunds and liability apply to wallet transactions, alongside authentication, fraud and complaints rules. The assessment should map MiCA safekeeping and reserve requirements against payment safeguarding obligations across issuance, custody and payment execution, identify any duplication or gap and propose targeted adjustments where evidenced. This is a request for assessment, rather than a conclusion that these rules necessarily conflict. Worked examples should also explain capital treatment. Recognition of equivalent protection is a reform recommendation and does not permit firms to disregard current cumulative requirements; and**
- **set out the sequence from the EBA's PSD2 approach to the new statutory exclusions and authorisation procedures, including treatment of pending applications, cross-border services and firms using an authorised payment-service partner. Temporary supervisory relief should not be described as a permanent exemption.**

The transition map should identify the interim PSD2 derogations in PSR Article 108a, which the April compromise would apply from entry into force under Article 112, ahead of general



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

application. Firms should be able to identify which exclusions and adjustments are available at each stage without repeating an authorisation exercise unnecessarily.

The EBA No-Action Letter transition ended on 2 March 2026. Its [Opinion of 12 February 2026](#) distinguishes authorised firms, pending applicants meeting specified conditions and firms required to cease relevant EMT payment services and offboard clients. Conditional continuation for pending applicants is supervisory advice, not a general exemption from authorisation. Firms must establish a lawful basis for their activities, including any appropriately authorised agency arrangement, and cannot rely on prospective PSD3/PSR changes as present permission. The review should focus on remaining duplication while retaining the protections needed by users of EMT payment services.

Part 4 - Topics beyond MiCA's current scope

Question 61. In case you consider the criteria for establishing whether a DeFi application is not fully decentralised not sufficiently clear, which of them should do you consider should be used to assess the degree of decentralisation?

The assessment should be multi-factor and should focus on functional control and intermediation. The strongest indicators are an identifiable person or coordinated group that can change essential rules, pause or upgrade the protocol, control access, dispose of user assets without the user's participation, determine transactions or fees, or otherwise perform a crypto-asset service on an ongoing basis. This is an indicator of practical control, not an exhaustive legal test for custody: divided keys and user participation require assessment of the parties' actual roles and any coordinated authority over assets.

Governance concentration is relevant where it produces practical control, including through delegated voting, retained token allocations, veto rights or dependence on a small group to execute approved changes. The ability to extract material fees or direct protocol revenue is also relevant because it can reveal both economic control and capacity to bear obligations. Marketing, brand stewardship or publication of code may support the analysis but should not, alone, make a person a regulated intermediary.

Open-source status is not a reliable proxy for decentralisation. Open code can remain centrally controlled; closed code can be deployed immutably without an administrator. Likewise, an emergency key should not automatically establish full control where its powers are narrowly constrained, transparent, time-limited and subject to independent multi-signature or governance checks. ESMA's examples should expressly recognise two possible rebuttals: powers narrowly reserved to meet an issuer's legal duties, such as pausing, freezing, allowlisting or implementing court-ordered transfers; and restrictions the owner places on its own assets, such as approval thresholds, allowlists or time delays. Neither should, by itself, be treated as evidence that a technology provider is an intermediary. The assessment should examine who sets and can change the restriction, its legal purpose and the discretion it confers; a compliance label should not conceal broader managerial control. Where intervention powers exist, disclosures should identify who can



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

exercise them, the permitted triggers and the controls on their use. Exercise of those powers should be auditable, with appropriate procedures for review and correction, without preventing lawful sanctions compliance or court-ordered action.

The Commission should distinguish the protocol, its developers and the services built around it. Publishing immutable software should not be regulated as if it were operating a financial intermediary. A person operating a managed interface, routing orders, selecting pools, providing custody or exercising discretionary control may be regulated for that activity even if the underlying protocol is decentralised.

ESMA should publish rebuttable indicators and examples rather than a binary checklist. The assessment should identify the person capable of compliance and the specific function for which it is responsible. This avoids imposing obligations on autonomous software or a diffuse community that has no legal or practical capacity to perform them.

Question 62. Do you believe that risks to users of fully decentralised DeFi protocols should be indirectly accounted for by MiCA, e.g. by requiring CASPs to conduct due diligence over DeFi protocols they connect their clients with, or in any other way?

Yes, but indirectly and only where a regulated intermediary actively selects, promotes, routes or integrates access for its clients. A CASP's obligation should reflect the service it controls. It should not become the guarantor of autonomous software, nor should neutral wallet or infrastructure functionality create strict liability for a protocol chosen independently by the user.

A CASP that recommends or provides a curated route to a protocol should conduct proportionate due diligence on governance and control, smart-contract and operational risk, administrator keys, custody, liquidity, oracle and bridge dependencies, audit history, material incidents and the quality of user disclosures. The assessment should be refreshed after material upgrades or incidents and should support clear risk warnings and access decisions. The record should include the technical restrictions applied at the point of access, such as the contracts and functions the CASP permits, checks run before a transaction is signed, and exposure limits per protocol. It should also record material changes to those controls and the reasons for exceptions, so that supervision can test the measures within the CASP's control.

Liability should follow failure to perform the regulated duty - for example, ignoring a known critical vulnerability, misrepresenting the scope of review or continuing to promote a protocol after a material change - rather than every loss occurring on the protocol. A common EU due-diligence standard and reliable records should provide rebuttable evidence of the steps taken, while preserving ongoing monitoring, supervisory scrutiny and liability for failures within the provider's responsibilities.

Access controls aimed at illicit finance should use documented, risk-based indicators and allow review; a public blacklist may be a useful signal but should not substitute for the CASP's assessment



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

or create an irrebuttable legal presumption. Rules should preserve access to global liquidity where the risks are understood and managed.

Question 62.1 Please specify how should MiCA account for risks from fully decentralised DeFi applications.

MiCA should combine proportionate CASP due diligence, standardised risk disclosure, monitoring of material changes and targeted access controls. Certification should provide rebuttable evidence of due diligence within its stated scope, rather than legal immunity or compulsory product authorisation for every permissionless protocol. A certificate should not displace a CASP's assessment of uncovered risks or its duty to respond to new information.

A certificate is necessarily point-in-time. It can test code, controls and disclosed performance, but it cannot guarantee future governance decisions, liquidity, oracle behaviour or composability with other protocols. Mandatory certification-only access would concentrate gatekeeping in certifiers, disadvantage open-source projects and risk giving users a false impression that losses are insured or prevented.

The better model is modular. Independent code and operational assurance should be recognised; CASPs should document how they use it, assess risks outside its scope and monitor changes. Higher-risk functions such as custody, leverage, complex bridges or concentrated oracle dependencies should receive enhanced review. Protocols with immutable, non-custodial functions and transparent risks should not be treated as equivalent to managed platforms merely because both are described as DeFi. Schemes should permit competing qualified assessors and equivalent independent evidence, so recognition does not concentrate access decisions in a small group of certifiers.

Question 63. Do you support introducing certification schemes for DeFi protocols and smart contracts?

GBBC supports voluntary, risk-based certification that can be relied upon as evidence within a CASP's due-diligence process. Certification should not replace authorisation where an identifiable operator performs a regulated service, and it should not become a mandatory licence for immutable software or every smart contract made available to the public.

Certification is most useful for functions where independent testing can materially reduce information asymmetry: custody or control of user assets, upgradeable contracts, bridges, complex oracle dependencies, leverage, liquidation mechanisms and protocols integrated or promoted by regulated intermediaries. A proportionate scheme could also recognise narrower code-security attestations for lower-risk, non-custodial components. These examples concern protocol functions. They should not be read as a basis for requiring certification of the software supplied by wallet, node or key-management providers merely because that software supports a protocol; the separate position on non-custodial wallet software is set out in Question 64.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Any recognised scheme should define the assurance scope, independence and competence of the certifier, testing methodology, materiality thresholds, expiry, monitoring of upgrades, incident disclosure and withdrawal of the certificate. The legal effect should be limited: a certificate should constitute rebuttable evidence of due diligence within its stated scope. It should neither guarantee performance nor displace ongoing monitoring or the duties of a person that controls or promotes the service. Schemes should accept existing independent security audits, SOC 2 Type II reports and ISO 27001 certification as evidence to the extent that their scope, currency and testing address the outcome being assessed. A provider should not have to repeat equivalent assurance work solely to obtain another certificate. Gaps specific to smart-contract behaviour or the relevant service should receive targeted testing rather than be assumed to be covered by a general organisational certification. Users should be able to verify the assessed contract address, network and software version, the assessment date and scope, and whether the certificate has expired or been withdrawn. Identifiers should link to accessible evidence; neither an identifier nor a certification mark should imply regulatory approval or guaranteed safety.

Question 64. Which of the following statements about potential certification schemes of DeFi protocols do you agree with?

GBBC's assessment of the four options is:

- Certification in place of CASP authorisation for a protocol that is not fully decentralised: strongly disagree. Where an identifiable operator performs a regulated service, a certificate cannot replace its authorisation and legal responsibilities. The software itself should not become the licence holder.
- Prescribed compliance tools as a condition of certification: rather disagree with a blanket technology prescription. Any voluntary scheme should test relevant outcomes and allow different technical means of achieving them. It should not require a developer to introduce control over user assets solely to qualify for certification.
- Mandatory certification before non-custodial wallet software is released: strongly disagree. Certification should not become a licence to publish software. A certificate cannot discharge custody, return or client-asset obligations that the developer has no capacity to perform.
- Incentives for certification of non-custodial wallet software: rather agree, provided participation is genuinely voluntary and the scheme is outcome-based, operated by accredited private bodies and open to reliance on existing independent audits and security certifications. Targeted additional testing should cover only relevant gaps; access to the market should not depend on obtaining the certificate.

Certification should state clearly which software version, controls and risks have been assessed. It should neither imply a guarantee against loss nor displace authorisation where the provider's actual activities constitute a regulated service. The same distinction between technical support and regulated activity should guide treatment of node and key-management software.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 77. If you identify any regulatory issue(s) in your answer to the previous question, please indicate what regulatory action is appropriate to address the issue(s) identified:

The Commission and EBA should confirm that a deposit recorded on DLT remains a deposit where its legal substance is unchanged and therefore remains outside MiCA. A bank's use of a technology provider to operate that record changes neither the nature of the depositor's claim nor the bank's responsibility. Classification should follow the rights and obligations created, rather than the ledger technology or the commercial label "deposit token".

Guidance should distinguish a deposit claim against a bank from an EMT or another transferable claim with different legal characteristics, and identify the facts that change the classification. Pure technology provision should not require CASP authorisation merely because it supports the bank's deposit service; any independently regulated activity must still be assessed on its own terms. Common, open identification and messaging standards should support verification of the issuing bank, the legal claim and its status across networks, without making access dependent on one provider's infrastructure. The Commission should assess technology-specific barriers to settlement and collateral use under CSDR and EMIR, including [EMIR Article 46](#). Eligibility should depend on enforceable rights, liquidity under stress and the relevant credit, market and operational risks; tokenisation or MiCA compliance alone should confer no entitlement to acceptance. Settlement arrangements should accommodate different forms of money where their distinct legal and risk characteristics meet the applicable requirements.

Question 78. Do tokenised deposits raise any specific issues under the CRD/CRR framework?

The starting point should remain the existing banking framework for an instrument that qualifies as a deposit. Supervisory guidance should make clear that using an external provider for ledger operation or signing infrastructure does not transfer the bank's responsibility for the deposit or its applicable prudential and operational obligations. The bank should demonstrate oversight, continuity and recoverability of the arrangement, while the provider's obligations should reflect its actual function. Tokenisation alone should not create an additional MiCA authorisation requirement for the deposit.

Question 80. Is there legal uncertainty as to the private law treatment of issuance, holding and transfers of tokens, under national law?

Yes. The uncertainty is not uniform across Member States or token structures, but it is material for cross-border transfer, third-party effectiveness, collateral, custody chains and insolvency. Regulatory authorisation under MiCA or MiFID does not itself determine who owns or is entitled to a token, whether a ledger transfer defeats competing claims or how client assets are treated if an intermediary fails.

The highest-significance and highest-urgency issues are the proprietary effect of transfer, recognition against third parties, good-faith acquisition, use as collateral, rights in intermediated



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

custody and treatment in insolvency. Recognition of tokens as objects of property and the distinction between native and non-native tokens are also important, but EU action should focus first on transactional outcomes rather than require Member States to adopt identical property-law concepts.

Issuance formalities are generally less urgent where sectoral legislation already defines the relevant process, although the legal link between a non-native token and the underlying asset must be enforceable. The answer may therefore differ by structure: for a native token the principal issue is the legal effect of control and transfer; for a tokenised financial instrument or other off-chain right, the framework must also determine whether transfer of the token transfers, evidences or merely instructs transfer of the underlying right.

Question 81. Would you recommend increasing the legal certainty in the treatment of tokens through EU law?

Yes. MiCA harmonises regulatory obligations, but it does not by itself determine ownership or entitlement, the proprietary effect of transfer, priority against third parties or the treatment of client tokens in insolvency. Those questions directly affect enforceability, collateral value and the ability to operate cross-border token markets.

There is a case for a targeted EU regulation establishing directly applicable rules for the proprietary outcomes needed in cross-border token markets, together with a coherent conflict-of-law regime. GBBC favours that instrument for the limited matters identified below, subject to a clear legal basis and an assessment of its interaction with national property and insolvency law. It need not replace Member State property law with a single abstract concept of token ownership. The framework must distinguish native crypto-assets from tokens recording rights governed by another body of law: for a tokenised bond, fund unit or claim, the law governing the underlying right remains relevant even where EU rules harmonise the effect of a ledger transfer.

Question 81.1. What are the 3 most important elements that should be addressed in EU law?

The three priority outcomes should be:

- **Transfer and third-party effect.** EU law should specify when a ledger entry transfers or evidences the relevant entitlement, when the transfer becomes effective against third parties and whether a good-faith acquirer is protected. For example, a purchaser receiving a token over a shared ledger should be able to determine whether an undisclosed prior disposition can defeat its claim. The Commission should also clarify the application of the [Settlement Finality Directive](#) to systems combining DLT and conventional records, distinguishing system designation, entry of transfer orders, irrevocability and insolvency protection. Ledger confirmation or use of a common rulebook should not alone be assumed to establish statutory finality. Where the asset and payment legs use different



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

systems, their rules should identify when each obligation is discharged and how a failed or delayed leg is managed.

- **Security interests and collateral.** The framework should provide predictable rules for creation, perfection, priority and enforcement of security interests over native tokens and tokenised rights. Market participants should know whether control of a wallet, an on-ledger notation or registration outside the ledger is required, and how competing claims rank.
- **Custody and insolvency.** EU law should clarify segregation, tracing, return and priority of client tokens where a custodian or intermediary enters insolvency, including omnibus and sub-custody structures. Operational control of a private key should not by itself determine beneficial entitlement or place client assets in the custodian's estate. This principle should also apply where a key is divided among several parties or a technology provider performs part of the signing process on the custodian's or client's instructions: participation alone should confer no beneficial entitlement. Where each client's assets are held at distinct addresses under distinct keys, the ledger can provide direct tracing rather than require reconstruction from an omnibus balance. EU law should recognise that arrangement as a method of client-asset segregation where reliable records link the addresses to the relevant client and the legal arrangements establish enforceable separation from the custodian's own estate. Technical separation and legal entitlement should be assessed together.

These outcomes should apply coherently across MiCA crypto-assets and DLT financial instruments, while preserving the additional investor and market-infrastructure protections applicable to financial instruments. The same ledger event should not have materially different proprietary consequences solely because the regulated wrapper changes.

Question 81.2 Can legal certainty (ownership or entitlement, transfer and enforceability of rights recorded as tokens) be achieved under EU law in one of the following manners?

The preferred approach is an EU conflict-of-law regime combined with partial harmonisation of the minimum proprietary outcomes needed for cross-border transactions. Full harmonisation of Member State property law would be disproportionate, while a standalone 28th regime may become useful only after its interaction with existing assets, insolvency and financial-market legislation is resolved. A new, targeted EU regulation is the preferred instrument for those common rules, with consequential amendments to existing regimes where needed, rather than stretching MiCA's regulatory perimeter to determine all private-law effects.

A conflict-of-law rule should use a predictable connecting-factor waterfall. It should begin with an accessible and valid choice in the token or system rules where that choice is not abusive and is visible to acquirers. If there is no valid choice, the rule should look to the law governing an identifiable system operator or register and then, for an issued token, to the issuer's establishment



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

or supervision. A final EU fallback is needed for native or decentralised assets with no issuer or administrator. Where a token records an underlying right, the law governing that right should continue to determine its existence and content, while the token rule governs the proprietary effect of the ledger transfer to the extent specified by EU law.

Partial harmonisation should then provide minimum rules on third-party effect, good-faith acquisition, collateral and client-asset protection in insolvency. This functional approach delivers the outcomes the market needs without forcing every Member State to adopt the same conceptual model of property.

A 28th regime should not be used as a shortcut around these questions. If developed, it should be optional, clearly bounded and interoperable with MiFID, MiCA, insolvency law, the Financial Collateral Directive and settlement-finality rules. It should not allow parties to opt out of mandatory investor protection or create two competing ownership systems for the same token.

Question 84. Should EU law introduce a conflict of law rule for tokens?

Yes. A harmonised conflict-of-law rule would produce immediate cross-border value even if Member States retain different concepts of ownership. It would allow issuers, holders, custodians, collateral takers and insolvency practitioners to identify in advance which law governs proprietary questions relating to a token.

Question 84.1 please explain why the current conflict of law rules applicable in EU are not enough or sufficiently clear in its application to tokens?

Existing EU rules are incomplete because several established connecting factors depend on the location of an asset, account, intermediary or register. A permissionless or distributed system may have nodes, developers, users and service providers in several jurisdictions without one location that determines the proprietary effects of transfer. The Financial Collateral Directive and Settlement Finality Directive also do not provide a complete answer for crypto-assets outside their scope or for structures that do not fit conventional account or register models.

The resulting uncertainty concerns more than the law of the issuer contract. It affects whether a transfer is effective against third parties, whether a good-faith acquirer is protected, how a security interest is perfected and which assets form part of an intermediary's insolvency estate. Divergent national answers can therefore arise from one ledger event even where the regulatory treatment under MiCA is harmonised.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 84.2 If the EU would introduce conflict of law rules for proprietary aspects of tokens, what would be the preferred connecting factors? Rank the below listed connection factors from 1 to 5 (1 being the most relevant connecting factor and 5 the least relevant connection factor). Connecting factors without a ranking will be considered not relevant:

The connecting factors should operate as a waterfall rather than as unrelated alternatives. GBBC would rank an accessible choice in the token first and a choice in the system rules second, provided the choice is visible, stable, valid under EU law and cannot be changed retrospectively to prejudice holders or third parties.

Where no valid choice exists, the next factors should be the law of a legally accountable system operator or supervised register, followed by the issuer's establishment or supervision where an issuer exists. The location of a technology provider should carry little weight unless that provider is itself the operator of the ledger system on which the token is recorded. The residence of a master-key holder is too operationally contingent to serve as a general connecting factor and could be manipulated or changed without altering the economic arrangement. The factor may also identify no single person in a threshold-signing arrangement: key material can be distributed across parties in different jurisdictions, with no party holding a usable complete key or able to act alone and no designated master-key holder. The location of one signing participant should not determine the law governing the token.

The list requires an additional fallback for a native token on a genuinely decentralised system with no issuer, operator, supervised register or master keyholder. EU legislation should supply a uniform default for that case, coordinated with the UNIDROIT Principles on Digital Assets and Private Law. The scope should cover proprietary effects, third-party effectiveness, priority, good-faith acquisition and collateral, while leaving the existence and content of an underlying off-chain right to the law otherwise governing that right