FREE RESOURCE

Is Your CASP AML Programme MiCA-Ready?

A Practical Checklist for MLROs and CCOs

This free checklist helps MLROs and CCOs assess their CASP AML programme against MiCA's authorisation requirements. It covers the six compliance areas that national competent authorities scrutinise most closely.

Score each question using the four-point scale below. Where your score is 1 or 2 in more than one area of any domain, that domain requires immediate attention ahead of your authorisation application.

This checklist draws on FATF's 2021 Virtual Assets guidance, MiCA Title VI, and the EU Transfer of Funds Regulation as applied to crypto-asset transfers.

MATURITY SCALE

1	**Not in place**	This control does not exist in any form. There is no policy, process, or system in place.
2	**Partially in place**	A control exists, but it has significant gaps: incomplete coverage, unclear ownership, or no review process.
3	**In place, not tested**	The control is in place and documented, but has not been independently tested or verified as effective.
4	**Effective and documented**	The control is in place, documented, regularly reviewed, and tested. You can trace it to a specific regulatory requirement.

Domain 1: Customer Due Diligence and KYC Lifecycle Management

Regulatory basis: FATF Recommendation 10 (Customer Due Diligence); MiCA Article 83; FATF 2021 Virtual Assets guidance, paragraphs 56-70.

Domain 1: CDD and KYC Lifecycle Management					
#	**Assessment Question**	**1**	**2**	**3**	**4**
1	Does your firm apply customer due diligence at onboarding that covers identity verification, beneficial ownership identification, and an initial risk rating? *FATF R.10; MiCA Art. 83*	1	2	3	4
2	Does your firm review and update customer risk ratings when specific risk indicators are detected, such as changes in transaction patterns, source-of-funds concerns, or adverse media? *FATF R.10; EBA Risk Factors Guidelines 2021*	1	2	3	4
3	Does your firm conduct periodic KYC refreshes at intervals proportionate to customer risk rating, with a defined frequency for high-, medium-, and low-risk customers? *FATF R.10; MiCA Art. 83(3)*	1	2	3	4
4	Does your firm apply Enhanced Due Diligence (EDD) for customers identified as higher risk, including PEPs, customers from high-risk jurisdictions, and customers with complex ownership structures? *FATF R.12-13; MiCA Art. 83(4)*	1	2	3	4
5	Can your firm demonstrate a clear audit trail for each CDD decision, including what was collected, when it was reviewed, and who made the risk rating decision? *FATF R.11; MiCA Title VI*	1	2	3	4

Domain 1 Total Score: _____ / 20

Domain 2: Transaction Monitoring

Regulatory basis: FATF Recommendation 10 and R.15 (Virtual Assets); MiCA Article 83; FATF 2025 Targeted Update priorities.

Domain 2: Transaction Monitoring					
#	**Assessment Question**	**1**	**2**	**3**	**4**
6	Does your firm's transaction monitoring cover risks specific to crypto assets, including stablecoin activity, DeFi protocol interactions, and unhosted wallet transactions? *FATF 2025 Targeted Update; FATF 2021 VA guidance*	1	2	3	4
7	Are your transaction-monitoring rules mapped to specific regulatory requirements and risk scenarios, with a documented rationale for each threshold? *FATF R.15; MiCA Art. 83*	1	2	3	4
8	Does your firm review and update transaction monitoring rules at defined intervals, or when the firm's products, customer base, or risk profile changes materially? *FATF R.15; FCA Dear CEO letter 2024*	1	2	3	4
9	Does your firm monitor for chain-hopping and layering patterns across multiple protocols or addresses, where funds are moved to obscure their origin? *FATF 2021 VA guidance, section 4*	1	2	3	4
10	Can your firm demonstrate that its transaction monitoring rules are calibrated to its actual risk profile, including volume thresholds adjusted for your specific customer base? *FATF R.10; MiCA Art. 83(2)*	1	2	3	4
11	Does your firm have a documented process for alert investigation, from initial alert through to SAR filing or case closure, with defined escalation routes? *FATF R.20; MiCA Title VI*	1	2	3	4

Domain 2 Total Score: _____ / 24

Domain 3: Sanctions Screening

Regulatory basis: FATF Recommendation 6 (Targeted Financial Sanctions); MiCA Article 83; EU sanctions framework (EU Regulation 2580/2001 and subsequent designations).

Domain 3: Sanctions Screening					
#	**Assessment Question**	**1**	**2**	**3**	**4**
12	Does your firm screen wallet addresses against OFAC, UN, and EU designated lists, in addition to named individual screening? *FATF R.6; INR.6; MiCA Art. 83*	1	2	3	4
13	Does your sanctions screening cover both the sending and receiving counterparty at the wallet address level for each transaction? *FATF 2021 VA guidance; FinCEN guidance*	1	2	3	4
14	Does your firm assess indirect sanctions exposure through chain analysis, identifying whether funds have passed through sanctioned addresses upstream? *FATF 2021 VA guidance, section 4*	1	2	3	4
15	Is your sanctions screening process documented, with defined procedures for handling a match, including escalation, freezing, and reporting obligations? *FATF R.6; EU sanctions framework*	1	2	3	4
16	Does your firm update its sanctions screening lists promptly when new designations are published, with a defined maximum lag time? *FATF R.6; EU Regulation 2016/1686*	1	2	3	4

Domain 3 Total Score: _____ / 20

Domain 4: Travel Rule Compliance

Regulatory basis: FATF Recommendation 16 (Wire Transfers), as applied to virtual assets; EU Transfer of Funds Regulation (TFR) extended to crypto-asset transfers; MiCA Article 83(3).

Domain 4: Travel Rule Compliance					
#	**Assessment Question**	**1**	**2**	**3**	**4**
17	Does your firm collect and transmit originator and beneficiary information for crypto-asset transfers as required by the EU Transfer of Funds Regulation? *FATF R.16; EU TFR 2023; MiCA Art. 83(3)*	1	2	3	4
18	Does your firm verify that counterparty VASPs are registered or licensed in their jurisdiction before processing transfers, using available registries? *FATF 2021 VA guidance; FATF VASP Implementation Table*	1	2	3	4
19	Does your firm have a documented procedure for handling transfers from non-compliant counterparties that fail to provide required originator or beneficiary information? *FATF R.16; EU TFR Article 12*	1	2	3	4
20	Does your firm conduct data quality checks on travel rule information received, identifying and acting on incomplete, inconsistent, or implausible data fields? *FATF Best Practice in Travel Rule Supervision 2025*	1	2	3	4
21	Is your travel rule compliance subject to periodic internal review, including testing of the data transmission mechanism and counterparty verification process? *FATF R.16; MiCA Art. 83*	1	2	3	4

Domain 4 Total Score: _____ / 20

Domain 5: Suspicious Activity Reporting

Regulatory basis: FATF Recommendation 20 (Reporting of Suspicious Transactions); MiCA Article 83; national FIU reporting obligations.

Domain 5: Suspicious Activity Reporting					
#	**Assessment Question**	**1**	**2**	**3**	**4**
22	Do your SARs include a specific, analytical narrative that explains why the activity is suspicious, rather than just repeating the alert trigger? *FATF R.20; national FIU guidance*	1	2	3	4
23	Does each SAR reference the specific risk indicators or red flags from FATF, MiCA, or other regulatory sources that the activity matches? *FATF 2021 VA guidance, red flag annex*	1	2	3	4
24	Does your firm have a defined SAR quality review process before submission, with a second reviewer or MLRO sign-off on higher-risk reports? *FATF R.20; MiCA Title VI*	1	2	3	4
25	Does your firm track SAR filing rates relative to alert volumes and review that ratio to ensure it reflects genuine risk-based decision-making? *FCA Dear CEO letter 2024; FATF R.20*	1	2	3	4
26	Does your firm maintain records of the investigation and reasoning behind all case closure decisions, including where a decision was taken not to file a SAR? *FATF R.11; MiCA Art. 83*	1	2	3	4

Domain 5 Total Score: _____ / 20

Domain 6: Governance and Oversight

Regulatory basis: FATF Recommendation 18 (Internal Controls and Foreign Branches); MiCA Articles 68-76; FATF 2021 VA guidance, section 5.

Domain 6: Governance and Oversight					
#	**Assessment Question**	**1**	**2**	**3**	**4**
27	Does the management body receive regular AML management information, including monitoring statistics, SAR volumes, alert disposition rates, and identified control weaknesses? *MiCA Art. 68; FATF R.18*	1	2	3	4
28	Does the MLRO have sufficient independence, standing, and resources to fulfil their obligations, including direct access to the management body without passing through a commercial function? *MiCA Art. 73; FATF R.18*	1	2	3	4
29	Has your firm reviewed its AML policies and procedures against MiCA's requirements and updated them to reflect the MiCA framework, not only the prior national regime? *MiCA Title VI; FATF 2021 VA guidance*	1	2	3	4
30	Does your firm conduct regular AML training for staff, including training on crypto-specific risk typologies such as stablecoins, DeFi, ransomware, and the travel rule? *MiCA Art. 72; FATF R.18*	1	2	3	4
31	Does your firm have a defined compliance calendar that includes periodic review of all AML controls, with ownership assigned to specific individuals? *MiCA Art. 68-76; FATF R.18*	1	2	3	4
32	Has your firm assessed its AML risk against its specific business model, customer base, jurisdictions, and products, and updated that risk assessment in the last 12 months? *MiCA Art. 83(2); FATF R.1*	1	2	3	4

Domain 6 Total Score: _____ / 24

Interpreting Your Results

Use your domain scores to identify where to focus your preparation.

Score Range	Assessment	Recommended Action
60% or below	Significant gaps identified across multiple domains	Prioritise a structured remediation plan immediately. Seek specialist support for your authorisation preparation.
61-80%	Partial readiness. Some controls are in place, but testing and documentation gaps remain.	Focus remediation on your lowest-scoring domains. Document the regulatory basis for each control before submitting your application.
81-100%	Strong foundation. Controls are in place and largely documented.	Validate remaining gaps and ensure all controls are traceable to specific regulatory requirements. Review before submitting your authorisation application.

Next Steps

If your score is 2 or below in more than two questions within any single domain, that domain should be your immediate priority.

A structured assessment of your AML programme against MiCA's requirements will give you a clear picture of your position and a prioritised roadmap for addressing any gaps.

Argus Pro has supported compliance teams across financial services, RegTech, and digital asset businesses in preparing for supervisory review. Our AFC framework covers the regulatory instruments that apply to CASPs under MiCA, and our assessment output is designed to support your authorisation application.

- A detailed gap analysis mapped to specific MiCA requirements
- An executive dashboard showing maturity across each compliance domain
- A traceability pack that maps each control finding to the relevant regulatory instrument
- A prioritised remediation roadmap

Speak to Argus Pro: info@arguspro.co.uk | +44 20 3996 3161 | arguspro.co.uk

Regulatory sources referenced in this checklist:

- Financial Action Task Force (FATF): Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021)
- Financial Action Task Force (FATF): Targeted Update on Implementation of FATF's Standards on Virtual Assets and VASPs (2025)
- European Parliament and Council: Markets in Crypto-Assets Regulation (MiCA), Regulation (EU) 2023/1114
- European Parliament and Council: Transfer of Funds Regulation as applied to crypto-assets, Regulation (EU) 2023/1113
- European Banking Authority (EBA): Guidelines on Customer Due Diligence and the Factors Credit and Financial Institutions Should Consider When Assessing the Money Laundering and Terrorist Financing Risk, 2021