31 January 2025
ESMA75-453128700-1263

Supervisory Briefing

Authorisation of CASPs under MiCA

Table of Contents

1 Executive Summary

Contents

ESMA has written a supervisory briefing for the use of NCAs to achieve a convergent approach in the EU to MiCA authorisation and is now publishing a shortened version of this briefing to provide orientation to market participants and the public at large. This supervisory briefing aims to assist NCAs in the practical application of requirements in the Market in Crypto Assets Regulation (MiCA) to the authorisation of crypto asset service providers (CASPs) and to promote harmonised authorisation practices throughout the Union.

The risk-based approach section describes the different risk factors that NCAs should consider in their approach to authorisation. CASPs to which (several of) these risk factors apply, should be subjected to an elevated level of scrutiny.

The sections on substance and governance, and outsourcing provide guidance on how NCAs should evaluate CASP substance and how they can determine whether CASP outsourcing arrangements are MiCA compliant. Reference is made to DORA and the high-level principles on third-party risk supervision as important elements to include in the evaluation of CASP outsourcing. Finally, guidance on the assessment of business plans of prospective CASPs is supplied.

2 Introduction

This document seeks to provide guidance and further promote supervisory convergence for the authorisation of Crypto Asset Service Providers (CASPs) under the Markets in Crypto Assets Regulation (MiCA). This supervisory briefing serves to further clarify the expectations regarding MiCA and translate them into concrete supervisory practices where needed to ensure a harmonised application. Interlinks with other areas, such as AML/CFT and ICT, are included, however, entities and NCAs should consult the relevant legal obligations, technical standards, and guidelines to ensure completeness.

3 Risk-based approach

3.1 Core principles/minimum thresholds

- ESMA is of the view that there are no low-risk CASPs. While the scale of CASPs' activity is typically less comprehensive compared to entities in traditional finance, CASPs often deal directly with retail investors and have a limited track record when it comes to regulatory compliance and supervision. They thus should be regarded as constituting a higher risk than entities operating in more mature sectors.
- There should therefore be no instances where a cursory assessment, based on a 'low-risk' categorisation, could exist.
- Instead, the use of a risk-based approach in the assessment of CASP applications should only result in elevated scrutiny for entities where above average risk might be expected given the presence of specific circumstances.
- The money laundering and terrorist financing risks (ML/TF) presented by CASPs are generally high. CASPs are exposed to ML/TF risks due to specific features of their business structure, the cross-border nature of their business and the technology used, which allows them to transfer crypto-assets instantly across the world and onboard customers in different jurisdictions. The risk is amplified when they process or facilitate transactions or offer products or services that present a higher degree of anonymity. As such, this is an area that deserves special attention. The EBA's ML/TF Risk factors Guidelines[1] provide further details on the ML/TF risks presented by CASPs and support for NCAs to assess that risk.

3.2 Key elements that create a higher risk

- **Size**. CASPs that are larger in size in terms of number of clients and amount of funds/assets have a potential for creating more harm in cases where they act in a way

[1] See Guidelines on ML/TF risk factors | European Banking Authority (europa.eu), Guidelines 21

that is non-compliant with MiCA. CASPs with more than 1.000.000 yearly active users[2] in the EU or a balance sheet size of €3.000.000.000 should be subjected to an elevated level of scrutiny. This does not prevent NCAs from subjecting smaller entities to an elevated level of scrutiny if they deem this appropriate in the context of their jurisdiction.

- **Complexity of group structure**. NCAs should be able to understand CASP group structures and corresponding responsibilities. Highly complex group structures involving a large number of entities, and/or with authorisations across legal frameworks (EMI/MiFID/CASP) create an elevated risk in several areas including: conflicts of interest, contagion, AML/CFT, and the ability for NCAs to effectively supervise the CASP. Consequently, CASPs with a complex group structure should be subjected to an elevated level of scrutiny.
- **Cross border activity**. A significant amount of cross-border activity creates an additional layer of risk and responsibility. Through the passporting regime, the choice to authorise a CASP affects consumers outside the home Member State. CASPs with more than 200.000 yearly active users outside the home Member State should be subjected to an elevated level of scrutiny. NCAs should pursue coordination with significant host NCAs to ensure concerns on a CASP's ability to meet MiCA standards in their service offering in host jurisdictions are identified as soon as possible (a host should be considered 'significant' where there are 100.000 or more yearly active users in the host Member State, and/or if the number of yearly active users in the host jurisdiction exceeds 50% of the total client base, and/or where the CASP operates a physical branch in the host Member State).
- **Role in ecosystem.** CASPs that play an important role in the crypto ecosystem constitute a higher level of risk, as they might negatively affect other CASPs if and when issues arise. Trading platforms and custody providers which provide services to other CASPs or that could otherwise be reasonably expected to create wider market fallout in case of issues should be subjected to an elevated level of scrutiny.
- **Combination of crypto-asset services.** CASPs that seek authorisation for a high number of CASP services potentially constitute a higher level or risk (and there is likely to be some overlap with the 'role in ecosystem' element listed above). These entities might function as Multifunction Crypto-asset intermediaries which have been flagged in the IOSCO report[3] as well as in the ESMA Opinion on Broker Models[4] as constituting relevant and unique risks. They should thus generally be subjected to an elevated level of scrutiny. The fact that different services carry with them different levels of risk should be taken into account[5].
- **Business model including combination of issuer and CASP activities.** New unique business models might constitute a higher risk. Amongst others, ART or EMT issuance combined with CASP services could create additional risks (amongst others with respect to conflicts of interest). As such an elevated level of scrutiny is warranted. This

[2] At least one trade in the last 12 months.
[3] FR11/23 Policy Recommendations for Crypto and Digital Asset Markets
[4] ESMA75-453128700-1048_Opinion_on_broker_models.pdf
[5] See also Annex IV MiCA

should at least include close coordination with relevant competent authorities, in particular where supervision of Issuers and CASPs is conducted by separate authorities.

- **Outsourcing of key functions.** Outsourcing can create additional operational risk. This includes intra-group outsourcing. The outsourcing of key functions, such as compliance personnel, risk personnel, key functions/staff required to operate ICT systems and related security arrangements should be subject to an elevated level of scrutiny.
- **Level of outsourcing.** NCAs should carefully consider whether the functions being outsourced are important to the compliant functioning of the CASP. While outsourcing of supporting roles (client or IT support below management level) might be possible without creating significant additional risk, outsourcing of more crucial roles should be subject to an elevated level of scrutiny. It should be noted that there are limits to the levels of outsourcing that can be accepted (see specific section on Outsourcing). Where outsourcing is at a level which raises concerns on the ability of the NCA to effectively supervise, an application should be rejected.
- **Type of outsourcing.** In addition to the previous point, outsourcing to third countries, including where this is intra-group outsourcing, can constitute an added operational risk. Among other things this might limit the ability for NCAs to effectively exercise their supervisory function. Consequently, CASPs that outsource work or functions to entities outside the EU should be subjected to an elevated level of scrutiny.
- **Supervisory history.** The supervisory history of an entity (including group entities and regulated subsidiaries), its shareholders, as well as its key function holders, should play a role in determining the level of scrutiny during authorisation. NCAs should namely consult the ESAs information system[6] (mandated under Articles 31a of the ESAs' founding regulations) to obtain relevant information. CASPs and/or key function holders that have been negatively assessed by other NCAs (including outside the EU), in the form of fines, warnings, being blacklisted, sanctions, supervisory reports, and ongoing investigations and procedures, should be subjected to an elevated level of scrutiny.

4 Substance and Governance

4.1 Core principles/minimum standards

- The local CASPs should have the power to autonomously make decisions on its EU policy. Reporting lines within the CASPs should demonstrate the ability to make such autonomous decisions at the EU level.
- Home NCAs should ensure that registered entities have sufficient in-country personnel and at least one executive management board member located in their jurisdiction. For

[6] This system holds limited information on persons who are subject to a fitness and propriety assessment under Union sectoral provisions. Competent authorities can refer to this system to identify other competent authorities that have conducted a previous fit and proper assessment on a specific person.

small Member States[7], allowances can be made for the executive management board member to be based in a different Member State, provided they are available at short notice (no more than 2 business days' notice) for ad-hoc in-person engagement with the NCA.

- Home NCAs should verify the decision-making powers and presence of executives and senior managers in the Member State. The burden of proof lies on CASPs. NCAs should be convinced that decision making does not lie elsewhere.
- A business set up where more functions are performed by or for the EU entity outside the EU than within it should be critically assessed. On assessing this, NCAs should look both at the number of functions performed outside the EU as well as the importance of these functions. Supporting functions (IT support, HR support) operating outside the EU might not prevent a robust and substantive operation within the EU. In addition, NCAs should consider the percentage of total costs that are spent on functions outside the EU as another indicator.
- NCAs should take a critical approach in determining if governance and substance arrangements interfere with the effective exercise of their supervisory function. This is particularly relevant in situations where:
    - the substance (on the management level and/or operational level) in the home jurisdiction is limited.
    - CASPs operate within a group structure with relevant group entities and/or group leadership operating outside the EU-regulatory scope.

4.2 Determining insufficient local autonomy

The following elements should be carefully considered when determining whether the CASP has sufficient local autonomy. This should be subject to the proportionality principle.

- The CASP should have an independent chair of the executive management board (dual-hatting with the parent company in case of a group entity should be limited and should not impair the independence of the chair)
    - A chair of the executive management board simultaneously operating in a management board role in the parent company of a group may interfere with the independent functioning of the EU-entity.
    - Dual hatting with the parent company within a group entity, especially one of considerable size and complexity, raises concerns on the ability to commit sufficient time.
- Executive management board members should be able to devote at least half of their time to the CASP.
    - Dual hatting should not impair the ability of executive management board members to effectively fulfil their responsibilities.

[7] Member States with fewer than 1 million inhabitants

- The chief executive officer should as a rule devote 100% of his/her time to his/her CASP duties. Only where NCAs are comfortable that this does not negatively impact the ability to effectively govern the CASP in a compliant manner, NCAs may allow lower time commitment. For members of the executive management board other than the CEO, NCAs can be more flexible on time commitment.
    - Executive management board composition and time commitment should reflect an executive management board that is able to operate effectively as a collective and is not dependent on one member.
- Executive management board members should possess strong local knowledge of both national and EU rules and context:
    - Executive management board members should be aware of national rules of the Member States in which it is located or provides a significant level of services.
    - Executive management board members should have knowledge of EU-market idiosyncrasies and awareness of the distinctive characteristics of the national market.
- On the basis of Article 59(2), recital 74, and recital 76, it should be understood that at least one of the CASP's executive management board members should be resident in the Union country where the authorisation is being granted or, in case of a small Member State, is based in a directly neighbouring country, provided they are available at short notice (no more than 2 business days' notice) for ad-hoc in-person engagement with the NCA.
    - Executive management board members should have relevant prior work experience (ideally in the same sector and ideally in the EU).
- There should be a significant local team present:
    - Key executive management board members and senior managers should be employed and present in the Member State of establishment proportionate to their role, ensuring they can effectively fulfil their responsibilities.
    - Sound governance and internal control mechanisms should provide clarity as to the allocation of responsibilities, documented policies and procedures which foster constructive challenge and the effective involvement of executive management board members/senior managers.
    - Outsourcing outside the home Member State can be justified where the staff based outside of the home jurisdiction consists primarily of staff in supporting roles (e.g. non-management level HR or IT support) and/or where the nature of the work to be undertaken outside of the home jurisdiction can be performed remotely without impairing the effectiveness thereof. Key roles should still be predominantly based within the home jurisdiction.
    - NCAs should be convinced that there is a clear ability to investigate and decide important EU-centric decisions within the CASP.
    - Management and key staff should be accessible to the home NCA.
- The EU-entity should have sufficient senior staff to be able to take decisions for the EU-level autonomously. Coordination at the group level is acceptable but should not reach the level where effective management lies outside the EU.

- The EU-entity representatives should be able to meet and discuss with the authorising NCA without the presence of a group representative and/or without 'taking the discussed points back to the (head) group entity for clearance'.
- The EU-entity executive management board should be able to exert significant influence on Group level decisions that affect the EU-entity.

4.3 Internal control function

- NCAs should ensure that responsibility for the compliance and risk function permanently rests with the CASP, which needs to be in charge of monitoring its own compliance risks.
- Combining the risk management or compliance management, with internal audit functions should be subjected to an elevated level of scrutiny as this may undermine their effectiveness and independence. For CASPs with a smaller size or lower risk profile, the risk management and compliance functions may be combined if keeping them separate would be disproportionate to the scale and complexity of their business activities.
- NCA should ensure that the internal control framework of a CASP allows for adequate identification, assessment and mitigation of ML/TF risks[8].
- The internal control framework should include a well-defined structure together with clear lines of roles and responsibilities. At least one executive management board member must be responsible for implementing, maintaining and monitoring the internal control and risk management framework to ensure effective oversight of these functions. Adequate segregation of duties must be established ensuring conflicting tasks and activities are not assigned to the same individual or team/function.
- The internal control framework should encompass the entire organisation, covering the activities (including regulated activities) of all business lines and internal units. Furthermore, the framework should also address outsourced activities to ensure that appropriate controls and oversight are applied to outsourcing arrangements. The internal control framework must at least include risk management, compliance, and internal audit functions.
- Comprehensive policies and procedures for compliance, internal audit (if required) and risk management should be established, including allocated roles and responsibilities, and workflows/instructions. These policies and procedures must include provisions regarding periodic reviews and updates when necessary to reflect changes in the regulatory environment and business operations.
- Policy and procedures should also include workflows that ensure submission to the executive management body of written reports on compliance and internal audit evaluations (at least once a year and on an ad hoc basis). CASPs should ensure that mechanisms are established to ensure that these deficiencies are reported to the

[8] Please also refer to EBA's 'Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849

executive management board in addition to assessing the identified deficiencies with the operational management.

4.4 Risk management framework.

- The risk management framework should incorporate comprehensive policies, procedures, clarify the risk appetite and establish limits, and controls to ensure effective and ongoing identification, measurement, assessment, monitoring, management, mitigation, reporting of risks, and evaluation. Components of the risk management framework should be as follows:
    - Roles and responsibilities: CASPs should designate key personnel, including risk managers, compliance officers[9], and internal auditors (if required), each with specific duties and accountabilities. Risk owners must be clearly defined to manage specific identified risks, implementing and maintaining appropriate risk controls. Responsibilities of second line (risk management) and internal audit must also be clearly defined. There should be adequate personnel within the CASPs to effectively manage and oversee outsourcing risks.
    - Risk appetite definition: CASPs should have a clearly defined risk appetite, which reflects the level of risk the organisation is willing to accept in line with its strategic goals. This appetite can be defined in terms of risk tolerance thresholds and acceptable risk levels or limits.
    - Risk identification: This should encompass not only integrity risks (such as AML/CFT[10] and fraud) but also ICT, operational, market, legal, compliance, conflicts of interests, and other relevant risks in accordance with all intended crypto-asset services. The risk identification process should address risks at various levels, including individual business lines and the overall entity together with outsourced activities. CASPs should maintain a risk register to systematically record identified risks and the actions taken to manage and mitigate them.
    - Risk assessment: CASPs should establish detailed approaches to assess risks, including both qualitative and quantitative methods. These methodologies could involve risk matrices, scenario analysis or stress testing, and statistical models to ensure a comprehensive evaluation. Risks should be categorised into various classes, such as high, medium, or low, based on their nature and impact. Good practice is to use good quality risk management tools.
    - Risk management: CASPs should develop specific actions and risk mitigation strategies to reduce or control risk exposure. For each individual risk identified, CASPs should develop targeted actions aimed at reducing the likelihood or impact of that specific risk together with assigning a risk owner who has sufficient mandate and knowledge in the risk area.

[9] See Guidelines on the role of AML/CFT compliance officers | European Banking Authority (europa.eu) for further detail
[10] See Guidelines on ML/TF risk factors | European Banking Authority (europa.eu)

- Monitoring and reporting: CASPs should implement systems and processes for continuous monitoring of risk management activities. The risk management framework must also include procedures for regularly reporting the status of risks and risk management activities to the management body. Reporting to the management body should also include proposed appropriate risk-mitigating actions.
- Evaluation: CASPs should conduct a comprehensive assessment of the risk management framework at least annually. This assessment should evaluate the framework's effectiveness, relevance, and adequacy in addressing emerging risks in line with CASPs' risk strategy and risk appetite. The scope of the assessment should include an examination of key risk management processes, controls, and procedures, as well as feedback from relevant stakeholders. Additionally, the assessment should consider any significant changes in the operational environment, regulatory requirements, or risk profile to determine if adjustments are needed.

4.5 Compliance function

- The compliance function ensures that the CASP adheres to external and internal rules. A strong, independent compliance function can mitigate risks related to misconduct, money laundering and other forms of non-compliance. Components of a sufficient compliance function are as follows:
  - Roles and responsibilities: sufficient mandate and clear working agreements with other stakeholders. Compliance should for example be involved in key strategic decision-making such as the choice of cooperating with third parties and selection of crypto-assets in relation to which to provide services. The compliance function should have sufficient independence, capacity, and competency to fulfil their responsibilities. CASPs should appoint at least one dedicated person to the compliance function (head of compliance or compliance officer). Only in rare exceptions, where appointing a dedicated head of compliance/compliance officer is evidently not proportionate to the business activities, can this role be combined with risk management tasks (second line).
  - Compliance plan: CASPs should develop yearly updated plans with appropriate compliance activities given the nature, scale and complexity of the business activities. There should be sufficient authority and adequate resources of the compliance function to perform these activities.
  - Monitoring and reporting: The compliance function identifies, assesses, advises on, monitors and reports on the CASPs compliance risk. Good practice is to use good quality compliance monitoring tools. The compliance function should undertake regular reporting, at least to the executive management board. There should be an escalation procedure in place to allow for reports to the supervisory board.

- Evaluation: CASPs should periodically (at least every year or where a material change in the composition and/or structure occurs, whichever precedes) evaluate if the compliance function is effective and if any adjustments are needed going forward.

- CASPs should comply with the EBA Guidelines on the role of AML/CFT compliance officers[11]

4.6 Dealing with staff outside the country of authorisation

- The use of staff outside the country of authorisation is acceptable but may impair the ability of the CASP to ensure continuity and regularity in the performance of their crypto-asset services. NCAs should therefore give due consideration to such an indication. The practice of employing staff outside the country of authorisation may need to be further restricted depending on the roles of the staff based outside the country of authorisation and/or the concentration of such staff at certain functions.
- In any case, using staff outside of the country of authorisation should not:
  - prevent the exercise of the supervisory functions of NCAs;
  - prevent prompt access to relevant information by the home NCA;
  - prevent management from exercising effective control over staff members;
  - undermine the capacity of CASPs to operate in a continuous and regular manner.

5 Outsourcing

5.1 Core principles/minimum standards

- Outsourcing arrangements should not involve the delegation of functions/services to an extent that the firm becomes a letter-box entity.
- Particular attention should be paid to the outsourcing of ICT infrastructure building/management. For the evaluation of these ICT third party risks NCAs should refer to DORA requirements.
- A situation where more functions are outsourced outside the EU than operated inside the EU should be carefully assessed. In assessing this, NCAs should look both at the number of functions performed outside the EU as well as the importance of these functions. The percentage of total costs that are spent on outsourced activities should be used as an indicator. Without prejudice to a case-by-case assessment, supporting functions (non-management level IT support, HR support) operating outside the EU might not prevent a robust operation within the EU.
- Outsourcing to jurisdictions where NCAs would be unable to obtain information from the entity to which work is outsourced is not compatible with Article 73(1)(d) of MiCA.

[11] See Guidelines on the role of AML/CFT compliance officers | European Banking Authority (europa.eu) for further detail

- CASPs should be able to demonstrate effective control over the activities they have outsourced. Among other things, this should be evidenced by having adequate personnel, i.e. adequate in number to reflect the level of outsourcing as well as adequate in terms of skills and experience within the CASPs to effectively manage and oversee outsourcing risks.
- Particular attention should be paid to the fact that the outsourcing of AML functions is restricted. Responsibility for AML compliance should always remain with the CASP.
- Comprehensive information should be provided by CASPs to ensure NCAs have sufficient knowledge and supervisory ability over outsourcing arrangements.
- Where CASPs intend to outsource functions/services to entities within the same corporate group, NCAs should assess the due diligence carried out by firms in more detail and be satisfied that the selection of a group entity is based on objective reasons. NCAs should also consider whether outsourcing to intra-group entities significantly affects the ability to make autonomous decisions on its EU activities. The best interest of EU activities should be the driving force for decisions, rather than adapting them to serve the benefits of other entities within the same group to which the service is outsourced.

5.2 Ensuring outsourcing does not result in the delegation of the responsibility of the crypto-asset service providers (article 73(1)(a)

- To ensure outsourcing does not result in the delegation of the responsibility by the CASP, NCAs should take into account:
    - The services/activities which are outsourced and their criticality to the functioning of the CASP (NCAs should refer to DORA where this involves ICT services).
    - The level of control the CASP can exercise over entities it engages with through outsourcing. Where such control is limited to the point a CASP is unable to supervise outsourced services effectively or is unable to manage the risks associated with the outsourcing, NCAs should not accept the arrangement.
    - The jurisdictions to which work is outsourced and the extent to which these prevent the NCA from exercising its supervisory authority (relation to Article 73(1)(d) of MiCA).
    - Whether entities to which work/activities are outsourced engage in further sub-outsourcing for critical and important operational functions provided to the CASP. Where this is the case this may create a higher risk of insufficient oversight and control at the CASP level.
    - Whether CASPs have a clear understanding of sub-outsourcing. To ensure good insight into the entire chain, the Service Level Agreement should ensure that the CASP has awareness off and control over sub-outsourcing.
- There is a risk that a single person could have insufficient knowledge, experience and time to monitor a broader range of services/functions in an effective manner. NCAs

should therefore engage critically with CASPs that intend to allocate the monitoring of a number of outsourced functions to a single person. NCAs should be satisfied that this does not raise additional risks to the soundness or continuity of services or to investor protection/market integrity.

5.3 Ensuring outsourcing does not prevent the exercise of the supervisory functions of competent authorities

- In some cases, outsourcing or delegation to a third-country entity requires prior cooperation agreements between the EU NCA and the third-country authority.
- NCAs should ensure that EU entities comply with governance requirements and can effectively control outsourced or delegated activities. This includes having the technical knowledge to request changes, monitor deployment, and assess service quality, i.e. the person directly employed by the CASP, responsible for specific outsourced activities should have sufficient knowledge/expertise of the activity or activities outsourced to allow for effective monitoring and control.
- NCAs should have effective access to all relevant data and business premises related to outsourced or delegated activities.

5.4 Outsourcing and custody

- Outsourcing the custody of client assets can only be done to entities that are authorised under Article 59 MiCA (see MiCA Article 75(9)) or those that are operating under a grandfathering period.

5.5 Outsourcing of ‘highly important’ functions

- Some activities, such as internal control, IT control, risk assessment, compliance, key management, and sector-specific functions require special scrutiny. While certain elements of such activities may be outsourced, outsourcing of these activities cannot be accepted if it jeopardises the regulated entities' activities and effective NCA supervision.
- NCAs should take careful note of outsourcing that may be precluded in light of AML rules.

6 Fit and proper Assessment

6.1 Core principles/minimum standards

- The complexity and relevance of the CASP in the overall crypto ecosystem should be considered when assessing individual and collective suitability. Consistent with the

section on ‘Risk-based approach’, CASPs that are larger, more complex and/or more crucial to the overall crypto ecosystem, require higher levels of specific skill and experience for executive board members.

6.2 Prior supervisory transgressions of executive management board members and supervisory board members

- NCAs should investigate prior supervisory violations, e.g. operating without the necessary registration in certain jurisdictions, even though the existence of such evidence should not necessarily result in a blanket inability for relevant board members to be deemed fit and proper.
- Board members with prior supervisory transgressions should be assessed on a case-by-case basis. To allow for effective testing it is important to:
    - Use the existence of prior EU or non-EU supervisory transgressions to potentially elevate the authorisation to a higher risk level (see also section on Risk-based approach).
    - Reach out to other relevant NCAs where transgressions (might) have taken place and incorporate their insights in the fit and proper testing.
    - Engage in personal interviews with such board members.
    - Assess whether board members demonstrate awareness of and learning from previous transgressions.

6.3 Interaction between collective suitability of an executive management board and individual deficiencies of executive management board members

- Technical knowledge is more relevant in the crypto asset ecosystem than in traditional finance. As such, all executive management board members must have at least a good level of understanding of the technical workings of crypto-assets and the crypto-asset services provided.
- Considering the nascent nature of the crypto-asset markets, executive management board members with less management experience can in principle be ‘compensated’ for by executive management board members with more management experience in the regulated finance industry.

6.4 F&P assessment where criminal proceedings are on-going

- NCA should take into account cases, both inside and outside the EU, where an entity, members of the management body, shareholders and persons, whether directly or

indirectly, that have qualifying holdings[12], are undergoing a criminal proceeding, even if a conviction or penalty is not imposed yet. This includes cases of guilty pleas amongst others.

- NCAs should also consult the AML/CFT CAs (including in future the EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism) and FIUs where appropriate[13]. Fit and proper assessments should be done on an on-going basis.

7 Business plan

Core principles/minimum standards

- The business plan should be realistic and should (if applicable) use current activities as a starting point for any projections.
- The business plan should contain realistic projections of activity over a three-year horizon with clearly defined intermediate points. The intermediate points should allow NCAs to monitor projections against reality.
- NCAs should require CASPs to consider how the continuity of their operation might be affected if revenues fall (well) below projections (i.e. pessimistic scenarios).

8 Notifications

8.1 Administration of notified MiCA services in national registers or dedicated sections of the NCAs' websites

- NCAs should create conditions in which clients are able to identify, in national registers or in a dedicated section of the NCA's official website, that an entity is allowed to provide crypto asset services (either as a MiCA authorised entity or through a notification). In addition, the national register or the relevant section of the NCA's official website should ideally allow clients to identify where an entity providing crypto asset services has been required to suspend services.

8.2 Incomplete notifications

- Entities wishing to notify crypto-asset services should inform NCAs 40 days before providing services for the first time. As per MiCA Article 60(8), NCAs should assess completeness of an application within 20 days of receiving a notification. In cases where the information provided is incomplete, an additional period of up to 20 days may

[13] Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units | European Banking Authority (europa.eu)

be allotted to collect the missing information. During this time the 40-day period is suspended. When the additional period expires, NCAs have 20 days remaining to check whether the notification is now complete. Where the notification is still incomplete after this time, NCAs should inform CASPs that the application remains incomplete and that they are **not** authorised to start providing the notified crypto-asset service(s). NCAs should also require the notifying entities to withdraw their notification and submit a new, complete application. This new application would then again be subjected to the timelines mentioned. This will help ensure a notification with clear and predictable timelines for both NCAs and notifying entities.