Baker McKenzie.

May 2024

MiCAR Compliance Toolkit

Guide to Authorization and Compliance Requirements for CASPs

Contents

Credit Institutions

I am a credit institution authorized in the EU under the Capital Requirements Directive (CRD).

1 Do I need to be authorized under MiCAR to provide cryptoasset services?

No. A credit institution does not need to separately apply for authorization under MiCAR to provide cryptoasset services in respect of in-scope cryptoassets. However, you will need to notify and provide certain information to your competent authority before providing these services for the first time.

Although this is a notification process, competent authorities will need to confirm that you have provided a complete notification before you can consider that the notification has been properly made.

Some regulatory engagement is therefore needed, although this should be less intensive than an authorization application.

2 Who do I need to notify?

The notification must be made to the competent authority in your home Member State – i.e. where you are authorized as a credit institution.

3 What information needs to be submitted?

The notification should include the following information:

- a program of operations setting out the types of cryptoasset services that you intend to provide, including where and how those services are to be marketed;
- a description of:
  - your internal control mechanisms, policies and procedures to ensure compliance with EU anti-money laundering (AML) requirements;
  - your risk assessment framework for the management of money laundering and terrorist financing risks; and
  - your business continuity plan;
- the technical documentation of your ICT systems and security arrangements, and a description of the same in non-technical language;
- a description of your procedure for the segregation of clients' cryptoassets and funds; and
- whether your cryptoasset service relates to asset-referenced tokens (ARTs), e-money tokens (EMTs) or other cryptoassets.

Other activity-specific information will need to be provided depending on the services you provide:

- Custody and administration of cryptoassets - a description of your custody and administration policy.
- Operating a trading platform for cryptoassets - a description of the operating rules of your trading platform and of your procedures and system to detect market abuse.
- Exchanging cryptoassets for funds or other cryptoassets - a description of your non-discriminatory commercial policy governing your relationship with clients as well as a description of your methodology for determining the price of the cryptoassets you propose to exchange for funds or other cryptoassets.
- Executing orders for cryptoassets on behalf of clients - a description of your execution policy.
- Advising on cryptoassets or providing portfolio management on cryptoassets - evidence that the natural persons giving advice on your behalf or managing portfolios on your behalf have the necessary knowledge and expertise to fulfil their obligations.
- Providing transfer services for cryptoassets on behalf of clients - information on the manner in which transfer services will be provided.

If you have previously provided this information to the authorities, then the notification can expressly state that the information previously provided remains up-to-date.

4 What form does the notification need to take

A harmonized template will be available. The European Supervisory Authorities (ESAs) are developing regulatory technical standards (RTS) on the information to be notified to competent authorities and implementing technical standards (ITS) on the standard forms, templates and procedures for the notification, including a standard form template of the notification to be submitted by financial institutions. These technical standards are expected to be finalized by 30 June 2024.

5 How long does the notification process take?

You will need to submit the notification at least 40 working days before providing cryptoasset services for the first time.

Don't forget the time it may take to prepare the information required – it is important to make sure that the notification is complete the first time to avoid delays and so you should make sure to build time into workplans to ensure that the notification is as complete as possible. We recommend allowing for 4-6 weeks to prepare the notification.

6 What is the assessment process?

After receipt of your notification, a competent authority must assess whether all required information has been provided within 20 working days of receipt.

If the competent authority concludes that your notification is not complete, it must notify you to provide the missing information within a timeframe that does not exceed 20 working days from the date of the request.

You must not begin providing the cryptoasset services while notification is still regarded as incomplete.

After the notification process is complete, information on your firm will be included on the European Securities and Markets Authority's (ESMA) publicly available register, which identifies cryptoasset service providers (CASPs), ART issuers, EMT issuers and cryptoasset white papers.

7 What regulatory and compliance requirements will I need to satisfy?

Not all requirements under MiCAR will apply to a credit institution. For example, authorization requirements and prudential requirements will not apply since credit institutions are already subject to these obligations under CRD.

As MiCAR closely follows the Markets in Financial Instruments Directive (MiFID) framework, credit institutions who are subject to and comply with MiFID in respect of financial instruments will be familiar with many of the compliance obligations under MiCAR.

As heavily regulated institutions, credit institutions should be well-placed to handle any compliance uplift as a result of MiCAR but should be careful to ensure that differences are addressed when preparing for MiCAR.

Some key areas of compliance are summarized below –
More information can be found in our **MiCAR Compliance Overview for CASPs** at the end of this Guide:

1. Governance arrangements –
Credit institutions are subject to governance requirements under MiCAR. These include ensuring that the management body and shareholders meet standards of good repute and ensuring that employees and managers are suitably skilled and knowledgeable. These should not have a material compliance burden given existing obligations that apply to CRD credit institutions.

2. Policies and procedures –
Policies and procedures will need to be updated with MiCAR-specific requirements.

3. Business continuity and operational resilience –
Credit institutions will need to have in place business continuity measures, which must comply with the Digital Operational Resilience Act (DORA).

4. Client communication and disclosures –
Complaints and customer disclosure policies will need to be updated for MiCAR. Disclosures around the environmental impact of cryptoasset activities will also be required.

5. Activity-specific obligations –
There are a number of activity-specific obligations that will apply depending on the cryptoasset activities that you perform – these include restrictions on third party payments when routing client orders in cryptoassets, obligations on the safeguarding of assets and contractual requirements.

6. Market Abuse –
MiCAR establishes a bespoke market abuse regime for cryptoassets, drawing on concepts in the Market Abuse Regulation (MAR), and prohibits insider dealing, unlawful disclosure of inside information and market manipulation. Market abuse policies and procedures will need to be updated with MiCAR requirements and staff will need to be trained on new obligations.

7. Significant CASPs –
A CASP must notify its competent authorities within two months of reaching the threshold where it has in the EU at least 15 million active users, on average, in one calendar year, where the average is calculated as the average of the daily number of active users throughout the previous calendar year. Such a CASP will be deemed significant – and as a result the competent authority must provide annual updates to ESMA on certain matters relating to the CASP.

8 As a credit institution, can I passport my cryptoasset services across the EU?

Yes. MiCAR amends the list of activities that can be passported under CRD to include:

- issuing e-money including issuing EMTs;
- the issuance of ARTs; and
- the cryptoasset services regulated by MiCAR.

MiFID Investment Firms

I am an investment firm authorized in the EU under MiFID.

1 Do I need to be authorized under MiCAR to provide cryptoasset services?

This depends on the cryptoasset services that you wish to undertake and the MiFID investment services and activities for which you are currently authorized.If you are already authorized to provide equivalent investment services and activities under MiFID, then separate authorization is not required under MiCAR.

However, you will need to notify and provide information to your Home State competent authority before providing MiCAR services for the first time. Although this is a notification process, competent authorities will need to confirm that you have provided a complete notification before you can consider that the notification has been properly made.

Some regulatory engagement is therefore needed, although this should be less intensive than an authorization application.

The MiCAR services and equivalent MiFID investment services/activities are set out in the table opposite - you should consider which MiCAR services you are providing and check that you hold the equivalent MiFID license.

If you are not specifically authorized to carry on MiFID investment services / activities that are equivalent to the cryptoasset service you wish you undertake, you will need to apply for full authorization under MiCAR, in addition to your existing MiFID authorization. See our Q&A below for **Entities Other than Credit Institutions, MiFID Investment Firms and EMIs** to find more information on the full authorization process.

In this Q&A we cover the notification process on the assumption that you hold the required authorizations under MiFID.

MiCAR service	Equivalent MiFID investment service / activity
Providing custody and administration of cryptoassets on behalf of clients	(Ancillary service) Safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management and excluding maintaining securities accounts at the top tier level
The operation of a trading platform for cryptoassets	Operation of a multilateral trading facility or operation of an organized trading facility (as applicable)
Exchange of cryptoassets for funds and other cryptoassets	Dealing on own account
Execution of orders for cryptoassets on behalf of clients	Execution of orders on behalf of clients
Placing of cryptoassets	Underwriting or placing of financial instruments on a firm commitment basis or placing of financial instruments without a firm commitment basis
Reception and transmission of orders for cryptoassets on behalf of clients	Reception and transmission of orders in relation to one or more financial instruments
Providing advice on cryptoassets	Investment advice
Providing portfolio management on cryptoassets	Portfolio management
Providing transfer services for cryptoassets on behalf of clients	No equivalent MiFID service or activity

2 Who do I need to notify?

The notification must be made to the competent authority in your home Member State – i.e. where you are authorized as an investment firm.

3 What information needs to be submitted?

The notification should include the following information:

- a program of operations setting out the types of cryptoasset services that you intend to provide, including where and how those services are to be marketed;
- a description of:
  - your internal control mechanisms, policies and procedures to ensure compliance with EU AML requirements;
  - your risk assessment framework for the management of money laundering and terrorist financing risks; and
  - your business continuity plan;
- the technical documentation of your ICT systems and security arrangements, and a description of the same in non-technical language;
- a description of your procedure for the segregation of clients' cryptoassets and funds; and
- whether your cryptoasset service relates to ARTs, EMTs or other cryptoassets.

Other activity-specific information will need to be provided depending on the services you provide:

- Custody and administration of cryptoassets - a description of your custody and administration policy.
- Operating a trading platform for cryptoassets - a description of the operating rules of your trading platform and of your procedures and system to detect market abuse.
- Exchanging cryptoassets for funds or other cryptoassets - a description of your non-discriminatory commercial policy governing your relationship with clients as well as a description of your methodology for determining the price of the cryptoassets you propose to exchange for funds or other cryptoassets.
- Executing orders for cryptoassets on behalf of clients - a description of your execution policy.
- Advising on cryptoassets or providing portfolio management on cryptoassets - evidence that the natural persons giving advice on your behalf or managing portfolios on your behalf have the necessary knowledge and expertise to fulfil their obligations.
- Providing transfer services for cryptoassets on behalf of clients - information on the manner in which transfer services will be provided.

If you have previously provided this information to the authorities then the notification can expressly state that the information previously provided remains up-to-date.

4 What form does the notification need to take

A harmonized template will be available. ESMA is developing RTS on the information to be notified to competent authorities and ITS on the standard forms, templates and procedures for the notification, including a standard form template of the notification to be submitted by financial institutions. These technical standards are expected to be finalized by 30 June 2024.

5 How long does the notification process take?

You will need to submit the notification at least 40 working days before providing cryptoasset services for the first time.

Don't forget the time it may take to prepare the information required – it is important to make sure that the notification is complete the first time to avoid delays and so you should make sure to build time into workplans to ensure that the notification is as complete as possible. We recommend allowing for 4-6 weeks to prepare the notification.

6 What is the assessment process?

After receipt of your notification, a competent authority must assess whether all required information has been provided within 20 working days of receipt.

If the competent authority concludes that your notification is not complete, it must notify you to provide the missing information within a timeframe that does not exceed 20 working days from the date of the request.

You must not begin providing the cryptoasset services while notification is still regarded as incomplete.

After the notification process is complete, information on your firm will be included on ESMA's publicly available register, which identifies CASPs, ART issuers, EMT issuers and cryptoasset white papers.

7 What regulatory and compliance requirements will I need to satisfy?

Not all requirements under MiCAR will apply to an investment firm. For example, authorization requirements and prudential requirements will not apply since investment firms are already subject to these obligations under MiFID and the IFD.

As MiCAR closely follows the MiFID framework, investment firms will be familiar with many of the compliance obligations under MiCAR.

As heavily regulated institutions, investment firms should be well-placed to handle any compliance uplift as a result of MiCAR but should be careful to ensure that differences are addressed when preparing for MiCAR.

Some key areas of compliance are summarized below –
More information can be found in our **MiCAR Compliance Overview for CASPs** at the end of this Guide:

1. Governance arrangements –
Investment firms are subject to governance requirements under MiCAR. These include ensuring that the management body and shareholders meet standards of good repute and ensuring that employees and managers are suitably skilled and knowledgeable. These should not have a material compliance burden given existing obligations that apply to MiFID investment firms.

2. Policies and procedures –
Policies and procedures will need to be updated with MiCAR-specific requirements.

3. Business continuity and operational resilience –
Investment firms will need to have in place business continuity measures, which must comply with DORA.

4. Client communication and disclosures –
Complaints and customer disclosure policies will need to be updated for MiCAR. Disclosures around the environmental impact of cryptoasset activities will also be required.

5. Activity-specific obligations –
There are a number of activity-specific obligations that will apply depending on the cryptoasset activities that you perform – these include restrictions on third party payments when routing client orders in cryptoassets, obligations on the safeguarding of assets and contractual requirements.

6. Market Abuse –
MiCAR establishes a bespoke market abuse regime for cryptoassets, drawing on concepts in MAR, and prohibits insider dealing, unlawful disclosure of inside information and market manipulation. Market abuse policies and procedures will need to be updated with MiCAR requirements and staff will need to be trained on new obligations.

7. Significant CASPs –
A CASP must notify its competent authorities within two months of reaching the threshold where it has in the EU at least 15 million active users, on average, in one calendar year, where the average is calculated as the average of the daily number of active users throughout the previous calendar year. Such a CASP will be deemed significant – and as a result the competent authority must provide annual updates to ESMA on certain matters relating to the CASP.

8 As an investment firm, can I passport my cryptoasset services across the EU?

Yes. If you intend to rely on the MiCAR passporting regime to provide services on a cross-border basis in more than one Member State, you must notify your home Member State competent authority by submitting the following information:

- a list of the Member States in which you intend to provide cryptoasset services;
- the specific cryptoasset services that you intend to provide on a cross-border basis;
- the starting date of the intended provision of the cryptoasset services; and
- a list of all other activities that you provide which are not covered by MiCAR.

The competent authority will, within 10 working days of receipt, communicate this information to the single points of contact of the host Member States, to ESMA and to the European Banking Authority (EBA), and will thereafter inform you of this communication. You may begin to provide cryptoasset services in other Member States from the date that you receive this communication, or at the latest from the 15th calendar day after having made the notification above.

Electronic Money Institutions

I am an e-money institution (EMI) authorized in the EU under the Second E-Money Directive (EMD2).

1 Do I need to be authorized under MiCAR to provide cryptoasset services?

This depends on the cryptoasset services that you wish to undertake and the types of cryptoassets supported by your services.

An EMI does not need to separately apply for authorization under MiCAR to provide cryptoasset services, provided that the cryptoasset services in question are the provision of custody and administration of cryptoassets on behalf of clients and the transfer services for cryptoassets on behalf of clients with regard to the EMTs that the EMI issues.

You will also still need to notify and provide certain information to your competent authority before providing these services for the first time.

If you wish to provide other types of cryptoasset services in respect of ARTs or other cryptoassets that are not EMTs (and no exemptions apply), you may need to apply for full authorization under MiCAR, in addition to your existing EMI authorization. See our Q&A below for **Entities Other than Credit Institutions, MiFID Investment Firms and EMIs** to find more information on the full authorization process.

2 Who do I need to notify?

The notification must be made to the competent authority in your home Member State – i.e. where you are authorized as an EMI.

3 What information needs to be submitted?

The notification should include the following information:

- a program of operations setting out the types of cryptoasset services that you intend to provide, including where and how those services are to be marketed;
- a description of:
  - your internal control mechanisms, policies and procedures to ensure compliance with EU AML requirements;
  - your risk assessment framework for the management of money laundering and terrorist financing risks; and
  - your business continuity plan;
- the technical documentation of your ICT systems and security arrangements, and a description of the same in non-technical language;
- a description of your procedure for the segregation of clients' cryptoassets and funds; and
- whether your cryptoasset service relates to ARTs, EMTs or other cryptoassets.

Other activity-specific information will need to be provided depending on the services you provide:

- Custody and administration of cryptoassets - a description of your custody and administration policy.
- Providing transfer services for cryptoassets on behalf of clients - information on the manner in which transfer services will be provided.

If you have previously provided this information to the authorities then the notification can expressly state that the information previously provided remains up-to-date.

4 What form does the notification need to take

A harmonized template will be available. ESMA is developing RTS on the information to be notified to competent authorities and ITS on the standard forms, templates and procedures for the notification, including a standard form template of the notification to be submitted by financial institutions. These technical standards are expected to be finalized by 30 June 2024.

5 How long does the notification process take?

You will need to submit the notification at least 40 working days before providing cryptoasset services for the first time.

Don't forget the time it may take to prepare the information required – it is important to make sure that the notification is complete the first time to avoid delays and so you should make sure to build time into workplans to ensure that the notification is as complete as possible. We recommend allowing for 4-6 weeks to prepare the notification.

6 What is the assessment process?

After receipt of your notification, a competent authority must assess whether all required information has been provided within 20 working days of receipt.

If the competent authority concludes that your notification is not complete, it must notify you to provide the missing information within a timeframe that does not exceed 20 working days from the date of the request.

You must not begin providing the cryptoasset services while notification is still regarded as incomplete.

After the notification process is complete, information on your firm will be included on ESMA's publicly available register, which identifies CASPs, ART issuers, EMT issuers and cryptoasset white papers.

7 What regulatory and compliance requirements will I need to satisfy?

Not all requirements under MiCAR will apply to an EMI. For example, authorization requirements and prudential requirements will not apply since EMIs are already subject to these obligations under EMD2.

However, EMIs intending to provide regulated cryptoasset services are likely to experience a more significant compliance uplift as a result of MiCAR, as the obligations under the regime are drawn from MiFID rather than EMD2. This may require careful planning and gap analysis to ensure that differences are addressed when preparing for MiCAR.

Some key areas of compliance are summarized below –
More information can be found in our **MiCAR Compliance Overview for CASPs** at the end of this Guide:

1. Governance arrangements –
Investment firms are subject to governance requirements under MiCAR. These include ensuring that the management body and shareholders meet standards of good repute and ensuring that employees and managers are suitably skilled and knowledgeable. These should not have a material compliance burden given existing obligations that apply to MiFID investment firms.

2. Policies and procedures –
Policies and procedures will need to be updated with MiCAR-specific requirements.

3. Business continuity and operational resilience –
Investment firms will need to have in place business continuity measures, which must comply with DORA.

4. Client communication and disclosures –
Complaints and customer disclosure policies will need to be updated for MiCAR. Disclosures around the environmental impact of cryptoasset activities will also be required.

5. Activity-specific obligations –
There are a number of activity-specific obligations that will apply depending on the cryptoasset activities that you perform – these include obligations on the safeguarding of assets and contractual requirements.

6. Market Abuse –
MiCAR establishes a bespoke market abuse regime for cryptoassets, drawing on concepts in MAR, and prohibits insider dealing, unlawful disclosure of inside information and market manipulation. Market abuse policies and procedures will need to be updated with MiCAR requirements and staff will need to be trained on new obligations.

7. Significant CASPs –
A CASP must notify its competent authorities within two months of reaching the threshold where it has in the EU at least 15 million active users, on average, in one calendar year, where the average is calculated as the average of the daily number of active users throughout the previous calendar year. Such a CASP will be deemed significant – and as a result the competent authority must provide annual updates to ESMA on certain matters relating to the CASP.

8 As an EMI, can I passport my cryptoasset services across the EU?

Yes. If you intend to rely on the MiCAR passporting regime to provide services on a cross-border basis in more than one Member State, you must notify your home Member State competent authority by submitting the following information:

- a list of the Member States in which you intend to provide cryptoasset services;
- the specific cryptoasset services that you intend to provide on a cross-border basis;
- the starting date of the intended provision of the cryptoasset services; and
- a list of all other activities that you provide which are not covered by MiCAR.

The competent authority will, within 10 working days of receipt, communicate this information to the single points of contact of the host Member States, to ESMA and to EBA, and will thereafter inform you of this communication. You may begin to provide cryptoasset services in other Member States from the date that you receive this communication, or at the latest from the 15th calendar day after having made the notification above.

Entities Other than Credit Institutions, MiFID Investment Firms and EMIs

I am an entity that is currently providing, or intends to provide in the future, services relating to cryptoassets in the EU.

1 Do I need to be authorized under MiCAR?

Yes. If you provide cryptoasset services within the EU, you will generally need to be authorized under MiCAR.

Once you are authorized under MiCAR in your home Member State, you will be able to passport your authorization throughout the EU - either through the right of establishment (e.g. via a branch structure) or on a services basis.

Exemptions are available under MiCAR (including a reverse solicitation exemption for overseas firms). You should carefully consider whether you require authorization or whether you may be able to rely on exemptions. Reverse solicitation is drawn narrowly under MiCAR.

Broadly, for mass retail business, it will be challenging to rely on exemptions for reverse solicitation – overseas firms will likely need to come onshore of the EU and be authorized under MiCAR to provide services to EU clients.

2 Is a grandfathering regime available for currently registered EU Virtual Asset Service Providers?

Entities already providing their cryptoasset services "in accordance with applicable law" before 30 December 2024 (commonly called virtual asset service providers (VASPs)) may continue to do so until 1 July 2026 or until they are granted or refused an authorisation, whichever is sooner. This should apply to VASPs registered under the EU AML regime, in addition to any national regulatory framework requirements, subject to Member State approach.

However, Member States have discretion to disapply this 18 month transitional period entirely, or to shorten its duration where they consider that their national regulatory framework is less strict than MiCAR. ESMA has called on Member States to consider limiting this transitional period to 12 months. Member States must confirm the transitional period to ESMA by 30 June 2024.

3 What is the deadline for authorization?

The authorisation requirements apply from 30 December 2024, unless you are able to benefit from a transitional period in your home Member State.

4 Where should I submit my application?

You will need to submit an application to the competent authority of your home Member State before providing cryptoasset services. Authorization must be granted before you commence any regulated services.

If you are a grandfathered EU VASP, ensure that you submit your application for MiCAR authorization prior to any deadlines specified by your national regulator.

If you do not yet have a physical presence in the EU, you should consider if you will need to incorporate an entity in the EU and employ relevant staff. To be authorized as a CASP:

- You must have a registered office in a Member State where you carry out at least part of their cryptoasset services.
- Your place of effective management must be in the EU and at least one of the directors must be resident in the EU.

5 What information needs to be submitted?

The application should include the following information:

- your name, including your legal name and any other commercial name used, your legal entity identifier, your website, a contact email address, a contact telephone number and your physical address;
- your legal form;
- your articles of association, where applicable;
- a program of operations, setting out the types of cryptoasset services that you intend to provide, including where and how those services are to be marketed;
- proof that you meet the applicable capital requirements;
- a description of your governance arrangements;
- proof that members of your management body are of sufficiently good repute and possess the appropriate knowledge, skills and experience required;
- the identity of any of your shareholders and members, whether direct or indirect, that have qualifying holdings and the amounts of those holdings, as well as proof that those persons are of sufficiently good repute;
- a description of:
  - your internal control mechanisms, policies and procedures to ensure compliance with EU AML requirements;
  - your risk assessment framework for the management of money laundering and terrorist financing risks; and
  - your business continuity plan;
- the technical documentation of your ICT systems and security arrangements, and a description thereof in non-technical language;
- a description of your procedure for the segregation of clients' cryptoassets and funds;
- a description of your complaints-handling procedures; and
- whether your cryptoasset service relates to ARTs, EMTs or other cryptoassets.

Other activity-specific information will need to be provided depending on the services you provide:

- Custody and administration of cryptoassets - a description of your custody and administration policy.
- Operating a trading platform for cryptoassets - a description of the operating rules of your trading platform and of your procedures and system to detect market abuse.
- Exchanging cryptoassets for funds or other cryptoassets - a description of your non-discriminatory commercial policy governing your relationship with clients as well as a description of your methodology for determining the price of the cryptoassets you propose to exchange for funds or other cryptoassets.
- Executing orders for cryptoassets on behalf of clients - a description of your execution policy.
- Advising on cryptoassets or providing portfolio management on cryptoassets - evidence that the natural persons giving advice on your behalf or managing portfolios on your behalf have the necessary knowledge and expertise to fulfil their obligations.
- Providing transfer services for cryptoassets on behalf of clients - information on the manner in which transfer services will be provided.

If you have previously provided this information to the authorities as part of an authorization under MiFID, EMD2 or the Payment Services Directive (PSD2), or local licensing requirements for VASPs prior to 29 June 2023, then the application can expressly state that the information previously provided remains up-to-date.

6 What form does the application need to take?

A harmonized template will be available. ESMA is developing RTS on the information to be notified to competent authorities and ITS on the standard forms, templates and procedures for the authorization application. These technical standards are expected to be finalized by 30 June 2024.

7 How long does the authorization process take?

You will need to submit your application before you take up the provision of any cryptoasset services. A competent authority must complete its assessment of your application and issue a fully reasoned decision granting or refusing authorization within 40 working days of receipt of your complete application, after which it has 5 working days to notify you of the decision.

Don't forget the time it may take to prepare the information required for your application pack – it is important to make sure that the application is complete the first time to avoid delays and so you should make sure to build time into workplans to ensure that the application is as complete as possible.
We recommend allowing for 12 weeks to prepare the application.

8 What is the assessment process?

After receipt of your application, a competent authority must assess whether all required information has been provided within 25 working days of receipt.

If the competent authority concludes that your application is not complete, it must notify you to provide the missing information within a specified timeframe.

When assessing your application, the competent authority will take into account the nature, scale and complexity of the cryptoasset services that you intend to provide.

If you are within the same group as, or are controlled by the same persons that control, an EU-regulated financial institution, the competent authority may consult the regulators in other relevant Member States.

A competent authority may refuse your application where there are objective and demonstrable grounds that:

- your management body poses a threat to your effective, sound and prudent management and business continuity, and to the adequate consideration of the interest of your clients and the integrity of the market, or exposes your firm to a serious risk of money laundering or terrorist financing;
- the members of your management body of and your shareholders/members that have qualifying holdings do not meet the relevant criteria (e.g. of sufficiently good repute, etc); or
- you fail to meet or are likely to fail to meet any MiCAR provisions applicable to CASPs.

Unless you are a grandfathered VASP providing services which you were previously registered to carry out, you must not begin providing the cryptoasset services or provide cryptoasset services outside of the scope of your grandfathering until you receive approval from the competent authority with respect to your authorization application.

After the notification process is complete, information on your firm will be included on ESMA's publicly available register, which identifies CASPs, ART issuers, EMT issuers and cryptoasset white papers.

9 What regulatory and compliance requirements will I need to satisfy?

MiCAR imposes significant compliance obligations based on the stringent requirements in MiFID that apply to investment businesses. We expect that this compliance environment may be unfamiliar to both new market entrants and VASPs currently operating under local regulations. As a result, firms intending to provide regulated cryptoasset services are likely to experience a significant compliance uplift as a result of MiCAR, even if they are currently registered as VASPs under local regulations. This will require careful planning and gap analysis when preparing for MiCAR.

Some key areas of compliance are summarized below –
More information can be found in our **MiCAR Compliance Overview for CASPs** at the end of this Guide:

1. Prudential requirements –
CASPs will need to hold minimum capital requirements at all times.

2. Governance arrangements –
CASPs are subject to governance requirements under MiCAR. These include ensuring that the management body and shareholders meet standards of good repute and ensuring that employees and managers are suitably skilled and knowledgeable. These obligations should be considered carefully, particularly by new market entrants and previously unlicensed firms.

3. Policies and procedures –
Policies and procedures will need to be updated with MiCAR-specific requirements.

4. Business continuity and operational resilience –
CASPs will need to have in place business continuity measures, which must comply with DORA.

5. Client communication and disclosures –
Complaints and customer disclosure policies will need to be updated for MiCAR. Disclosures around environmental impact of cryptoasset activities will also be required.

6. Activity-specific obligations –
There are a number of activity-specific obligations that will apply depending on the cryptoasset activities that you perform – these include restrictions on third party payments when routing client orders in cryptoassets, obligations on the safeguarding of assets and contractual requirements.

7. Market Abuse –
MiCAR establishes a bespoke market abuse regime for cryptoassets, drawing on concepts in MAR, and prohibits insider dealing, unlawful disclosure of inside information and market manipulation. Market abuse policies and procedures will need to be updated with MiCAR requirements and staff will need to be trained on new obligations.

8. Significant CASPs –
A CASP must notify its competent authorities within two months of reaching the threshold where it has in the EU at least 15 million active users, on average, in one calendar year, where the average is calculated as the average of the daily number of active users throughout the previous calendar year. Such a CASP will be deemed significant – and as a result the competent authority must provide annual updates to ESMA on certain matters relating to the CASP.

9. Changes in control –
Changes in control over specified thresholds will need to be notified to and assessed by the competent authority.

10 As an authorized CASP, can I passport my cryptoasset services across the EU?

Yes. If you intend to rely on the MiCAR passporting regime to provide services on a cross-border basis in more than one Member State, you must notify your home Member State competent authority by submitting the following information:

- a list of the Member States in which you intend to provide cryptoasset services;
- the specific cryptoasset services that you intend to provide on a cross-border basis;
- the starting date of the intended provision of the cryptoasset services; and
- a list of all other activities that you provide which are not covered by MiCAR.

The competent authority will, within 10 working days of receipt, communicate this information to the single points of contact of the host Member States, to ESMA and to EBA, and will thereafter inform you of this communication.

You may begin to provide cryptoasset services in other Member States from the date that you receive this communication, or at the latest from the 15th calendar day after having made the notification above.

MiCAR Compliance Overview for CASPs

General ongoing regulatory and compliance obligations

What general ongoing regulatory and compliance requirements will I need to satisfy?		Do these obligations apply to my firm?			
Compliance obligation	**Description**	**Credit institution**	**Investment firm**	**EMI**	**CASP**
Acting in clients' best interests	CASPs must act honestly, fairly and professionally in accordance with the best interests of their clients and prospective clients.	YES ✓	YES ✓	YES ✓	YES ✓
Prudential requirements	CASPs must adhere to minimum capital requirements.	NO ✗ You must continue to comply with the requirements applicable to CRD credit institutions – e.g. under the CRR.	NO ✗ You must continue to comply with the requirements applicable to MiFID investment firms – e.g. under the CRR or the IFR, as the case may be.	NO ✗ You must continue to comply with the requirements applicable to EMIs – e.g. under EMD2.	YES ✓ CASPs must, at all times, have in place prudential safeguards equal to an amount of at least the higher of the following: ▪ the amount of permanent minimum capital requirements specified in MiCAR, depending on the type of the cryptoasset services provided (ranging from EUR 50,000 to EUR 150,000); ▪ one quarter of the fixed overheads of the preceding year, reviewed annually – calculated in accordance with prescribed criteria and items. The prudential safeguards can take the form of own funds (in accordance with CRR requirements) and/or an insurance policy covering the EU territories where cryptoassets services are provided that includes certain prescribed characteristics and coverage (or a comparable guarantee).

What general ongoing regulatory and compliance requirements will I need to satisfy?		Do these obligations apply to my firm?			
Compliance obligation	**Description**	**Credit institution**	**Investment firm**	**EMI**	**CASP**
Governance arrangements	Members of the management body should: ▪ be of sufficiently good repute and possess the appropriate knowledge, skills and experience to perform their duties (in particular, they must not have been convicted of any money laundering or terrorist financing offences); and ▪ demonstrate that they are capable of committing sufficient time to effectively perform their duties. Shareholders and members that have direct or indirect qualifying holdings in the firm (i.e. persons holding at least 10% of the capital or of the voting rights in or is able to exercise a significant influence over the management of the CASP) are also expected to be of sufficiently good repute and, in particular, must not have been convicted of offences relating to money laundering or terrorist financing. CASPs should employ personnel with the necessary knowledge, skills and expertise, taking into account the scale, nature and range of cryptoasset services provided.	YES ✓	YES ✓	YES ✓	YES ✓
Policies and procedures	CASPs are required to adopt policies and procedures that are sufficiently effective to ensure compliance with the relevant provisions of MiCAR, which must be assessed and periodically reviewed by the management body and appropriate measures must be taken to address any deficiencies.	YES ✓	YES ✓	YES ✓	YES ✓
Business continuity and operational resilience	CASPs must take all reasonable steps to ensure continuity and regularity in the performance of cryptoasset services, and employ appropriate and proportionate resources and procedures including resilient and secure ICT systems as required by DORA. A business continuity policy must be established, which must include ICT business continuity plans as well as ICT response and recovery plans set up pursuant to DORA. This should aim to ensure, in the case of an interruption to their ICT systems and procedures, the preservation of essential data and functions and the maintenance of cryptoasset services or, where that is not possible, the timely recovery of such data and functions and the timely resumption of cryptoasset services. Systems and procedures must be established to safeguard the availability, authenticity, integrity and confidentiality of data pursuant to DORA.	YES ✓	YES ✓	YES ✓	YES ✓

What general ongoing regulatory and compliance requirements will I need to satisfy?		Do these obligations apply to my firm?			
Compliance obligation	**Description**	**Credit institution**	**Investment firm**	**EMI**	**CASP**
Record-keeping requirements	Records must be kept of all cryptoasset services, activities, orders, and transactions undertaken by CASPs. The records must be kept for a period of 5 years or, where requested by the competent authority, up to 7 years.	YES ✓	YES ✓	YES ✓	YES ✓
AML/CFT	MiCAR does not create a bespoke AML/CFT framework for CASPs. This is covered by the MLD and the revised Wire Transfer Regulation (WTR), which CASPs will need to comply with. CASPs are required to put in place effective procedures and arrangements for risk assessment, to comply with MLD. The adequacy and effectiveness of those mechanisms, systems and procedures must be monitored and evaluated on a regular basis, taking into account the scale, the nature and range of cryptoasset services provided, and appropriate measures must be taken to address any deficiencies. CASPs must comply with the revised WTR – i.e. among other things, CASPs must collect and make accessible certain information on the sender and recipient of cryptoasset transfers in relation to which they provide services (similar to the regime in place with respect to payment service providers / banks and wire transfers).	YES ✓	YES ✓	YES ✓	YES ✓
Complaints	CASPs must establish and maintain effective and transparent procedures for the prompt, fair and consistent handling of complaints received from clients. CASPs must also publish a description of these procedures. Clients must be able to file complaints free-of-charge.	YES ✓	YES ✓	YES ✓	YES ✓
Conflicts of interest	CASPs must implement and maintain effective policies and procedures, taking into account the scale, the nature and range of cryptoasset services provided, to identify, prevent, manage and disclose conflicts of interest. Conflicts of interest must be disclosed prominently on the CASP's website.	YES ✓	YES ✓	YES ✓	YES ✓

What general ongoing regulatory and compliance requirements will I need to satisfy?		Do these obligations apply to my firm?			
Compliance obligation	**Description**	**Credit institution**	**Investment firm**	**EMI**	**CASP**
Protection of client assets	CASPs holding cryptoassets belonging to clients or the means of access to such cryptoassets must make adequate arrangements to safeguard the ownership rights of clients, especially in the event of insolvency, and to prevent the use of clients' cryptoassets for the CASP's own account. CASPs providing payment services in relation to the cryptoasset services must make certain disclosures to their clients about the terms and conditions of those services, and whether they are provided directly or by a third party.	YES ✓ Further, with respect to any client funds received, you must comply with relevant obligations that apply to you as a credit institution.	YES ✓ Further, with respect to any client funds received, you must comply with client money protection provisions that apply to you as an investment firm.	YES ✓ Further, with respect to any client funds received, you must comply with safeguarding provisions that apply to you as an EMI.	YES ✓ The following requirements also apply: If your business involves holding client funds (i.e. fiat monies, not including EMTs), you are required to make adequate arrangements to safeguard the ownership rights of clients, and prevent the use of clients' funds for your own account. In particular, CASPs must, by the end of the business day following the day on which clients' funds (other than EMTs) were received, place those funds with a credit institution or a central bank. CASPs must also take all necessary steps to ensure that such clients' funds held with a credit institution or a central bank are held in an account separately identifiable from any accounts used to hold funds belonging to the CASPs.
Outsourcing	CASPs must have a policy on their outsourcing, including on contingency plans and exit strategies, taking into account the scale, the nature and the range of crypto-asset services provided. Outsourcing arrangements must be defined in a written agreement setting out the rights of CASPs and of the third parties to which they are outsourcing. Outsourcing agreements must give CASPs the right to terminate those agreements.	YES ✓	YES ✓	YES ✓	YES ✓

What general ongoing regulatory and compliance requirements will I need to satisfy?		Do these obligations apply to my firm?			
Compliance obligation	**Description**	**Credit institution**	**Investment firm**	**EMI**	**CASP**
Client communication and disclosures	CASPs must provide their clients with information that is fair, clear and not misleading, including in marketing communications, which must be identified as such. CASPs must not, deliberately or negligently, mislead a client in relation to the real or perceived advantages of any cryptoassets, and must warn clients of the risks associated with transactions in cryptoassets. CASPs must make publicly available, in a prominent place on their website: ▪ policies on pricing, costs and fees; and ▪ information related to the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue each cryptoasset in relation to which they provide services. That information may be obtained from the cryptoasset white papers.	YES ✓	YES ✓	YES ✓	YES ✓
Market abuse	MiCAR establishes a bespoke market abuse regime for cryptoassets, drawing on concepts in MAR, and prohibits insider dealing, unlawful disclosure of inside information and market manipulation. CASPs must also comply with requirements relating to systems, procedures and arrangements to monitor and detect market abuse.	YES ✓	YES ✓	YES ✓	YES ✓
Significant CASPs	ASPs must notify their competent authorities within two months of reaching the threshold where it has in the EU at least 15 million active users, on average, in one calendar year, where the average is calculated as the average of the daily number of active users throughout the previous calendar year. These CASP will be deemed significant – and as a result the competent authority must provide annual updates to ESMA on certain matters relating to the CASP.	YES ✓	YES ✓	YES ✓	YES ✓

What general ongoing regulatory and compliance requirements will I need to satisfy?		Do these obligations apply to my firm?			
Compliance obligation	**Description**	**Credit institution**	**Investment firm**	**EMI**	**CASP**
Change in control requirements	Changes in control will need to be notified to and assessed by the competent authority.	YES ✓ Assessed in accordance with CRD requirements.	YES ✓ Assessed in accordance with MiFID requirements.	YES ✓ Assessed in accordance with EMD2 requirements.	YES ✓ Changes in control over specified thresholds in respect of a CASP will need to be notified to and assessed by the competent authority. The notification requirement applies to any person or persons acting in concert that intends, directly or indirectly, to acquire or dispose, or to increase or decrease, a qualifying holding so that: ▪ the proportion of the voting rights or of the capital held would reach or exceed / fall below 20%, 30% or 50%; or ▪ the CASP would become or cease to be its subsidiary.

Ongoing regulatory and compliance obligations applying to specific cryptoasset services

Specific cryptoasset service	Compliance obligations
Custody and administration of assets	CASPs providing custody and administration of cryptoassets on behalf of clients must: ▪ conclude an agreement with their clients to specify their duties and their responsibilities, and include certain provisions in the agreement; ▪ keep a register of positions, opened in the name of each client, corresponding to each client's rights to the cryptoassets; and ▪ establish a custody policy with internal rules and procedures to ensure the safekeeping or the control of such cryptoassets, or the means of access to the cryptoassets.
Operating a trading platform	CASPs operating a trading platform for cryptoassets must: ▪ lay down, maintain and implement clear and transparent operating rules for the trading platform, which cover certain prescribed minimum areas (e.g. approval process; customer due diligence; exclusion categories; policies, procedures and the level of fees, if any, for the admission to trading; set objective, non-discriminatory rules and proportionate criteria for participation in the trading activities, which promote fair and open access to the trading platform for clients willing to trade, and conditions for cryptoassets to remain accessible for trading, including liquidity thresholds and periodic disclosure requirements, and conditions under which trading of cryptoassets can be suspended); ▪ assess the suitability of any cryptoassets before admitting them to trading; ▪ not deal on own account on the trading platform for cryptoassets they operate, including where they provide the exchange of cryptoassets for funds or other cryptoassets; and ▪ provide their clients with hyperlinks to any cryptoasset white papers for the cryptoassets in relation to which they are operating a trading platform.
Exchanging cryptoassets for funds or other cryptoassets	CASPs exchanging cryptoassets for funds or other cryptoassets must: ▪ establish a non-discriminatory commercial policy that indicates, in particular, the type of clients they agree to transact with and the conditions that shall be met by such clients; and ▪ publish a firm price of the cryptoassets or a method for determining the price of the cryptoassets that they propose to exchange for funds or other cryptoassets, and any applicable limit determined by that cryptoasset service provider on the amount to be exchanged; and ▪ provide their clients with hyperlinks to any cryptoasset white papers for the cryptoassets in relation to which they providing exchange services.
Executing orders for cryptoassets on behalf of clients	CASPs executing orders for cryptoassets on behalf of clients must take all necessary steps to obtain, while executing orders, the best possible result for their clients taking into account factors of price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the cryptoassets or any other consideration relevant to the execution of the order.

Specific cryptoasset service	Compliance obligations
Receiving and transmitting orders for cryptoassets on behalf of clientss	CASPs receiving and transmitting orders for cryptoassets on behalf of clients must: ▪ establish and implement procedures and arrangements that provide for the prompt and proper transmission of client orders for execution on a trading platform for cryptoassets or to another CASP; and ▪ not receive any remuneration, discount or non-monetary benefit in return for routing orders received from clients.
Placing cryptoassets	CASPs placing cryptoassets must: ▪ communicate certain information to the offeror, to the person seeking admission to trading, or to any third party acting on their behalf, before entering into an agreement with them, and agree on this information before placing those cryptoassets; and ▪ ensure that its rules on conflicts of interest have specific and adequate procedures in place to identify, prevent, manage and disclose any conflicts of interest arising from specific placement situations.
Providing advice on cryptoassets or providing portfolio management of cryptoassets	CASPs providing advice on cryptoassets or providing portfolio management of cryptoassets must ▪ assess whether the cryptoasset services or cryptoassets are suitable for their clients or prospective clients, taking into consideration their knowledge and experience in investing in cryptoassets, their investment objectives, including risk tolerance, and their financial situation including their ability to bear losses; and ▪ provide their clients with hyperlinks to any cryptoasset white papers for the cryptoassets in relation to which they are providing advice or portfolio management.
Providing transfer services for cryptoassets on behalf of clients	CASPs providing transfer services for cryptoassets on behalf of clients must conclude an agreement with their clients to specify their duties and their responsibilities, and include certain provisions in the agreement.

Key contacts

United Kingdom

Mark Simpson
Partner
Mark.Simpson
@bakermckenzie.com

Melody Hoay
Associate
Melody.Hoay
@bakermckenzie.com

Sarah Williams
Associate
Sarah.Williams
@bakermckenzie.com

Kimberly Everitt
Senior
Knowledge Lawyer
Kimberly.Everitt
@bakermckenzie.com

Austria

Robert Wippel
Counsel
Robert.Wippel
@bakermckenzie.com

Belgium

Olivier
Van den broeke
Associate
Olivier.Vandenbroeke
@bakermckenzie.com

Czech Republic

Jan Kolar
Associate
Jan.Kolar
@bakermckenzie.com

France

Iris Barsan
Counsel
Iris.Barsan
@bakermckenzie.com

Elisa Deuffic
Associate
Elisa.Deuffic
@bakermckenzie.com

Germany

Manuel Lorenz
Partner
Manuel.Lorenz
@bakermckenzie.com

Conrad Ruppel
Partner
Conrad.Ruppel
@bakermckenzie.com

Manuel Metzner
Counsel
Manuel.Metzner
@bakermckenzie.com

Hungary

József Vági
Partner
Jozsef.Vagi
@bakermckenzie.com

Italy

Eugenio Muschio
Partner
Eugenio.Muschio
@bakermckenzie.com

Luxembourg

Catherine Martougin
Partner
Catherine.Martougin
@bakermckenzie.com

Netherlands

Tim Alferink
Partner
Tim.Alferink
@bakermckenzie.com

Willem van Rees
Associate
Willem.vanRees
@bakermckenzie.com

Poland

Jerzy Bombczynski
Counsel
Jerzy.Bombczynski
@bakermckenzie.com

Spain

Paula De Biase
Partner
Paula.DeBiase
@bakermckenzie.com

Javier Portillo
Associate
Javier.Portillo
@bakermckenzie.com

Berta Satrustegui
Associate
Berta.Satrustegui
@bakermckenzie.com

Yves Mauchle
Partner
Yves.Mauchle
@bakermckenzie.com

Switzerland

Ansgar Schott
Partner
Ansgar.Schott
@bakermckenzie.com

Check out the other guides in our **MiCAR Compliance Toolkit**

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com