

Expand into Crypto-Assets with MiCAR

What it means for Cyprus Investment Firms?



The Markets in Crypto-Assets Regulation (MiCAR) introduces a harmonised EU framework for crypto-assets, enhancing investor protection and market integrity. Under MiCAR, Cyprus Investment Firms (CIFs) can leverage their existing license under Law 87(I)/2017 to offer regulated crypto-asset services. CIFs can combine traditional investment services with crypto offerings and passport them across the EU, unlocking opportunities within a unified regulatory environment.

Q&A:

1. Do CIFs need a separate MiCAR authorisation?

Generally, no. Cyprus Investment Firms (CIFs) may offer crypto-asset services without obtaining a separate MiCAR licence, provided these services are equivalent to those already covered under their existing CIF authorisation. Under Article 60 of MiCAR, CIFs are deemed Crypto-Asset Service Providers (CASP) and may offer equivalent services via a notification to CySEC, without requiring additional approval. This reflects their compliance with MiFID II and existing regulatory oversight. However, according to the European Commission's clarification (ESMA Q&A 2125), entities falling under Articles 60(2)–(6) of MiCAR may also apply

for a CASP authorisation under Article 62, if they intend to provide crypto-asset services not considered equivalent under Article 60.

□ Next steps

Review your current CIF permissions to assess whether they align with the intended crypto-asset services (see mapping table below).

- Where alignment exists, a notification to CySEC is sufficient.
- Where it does not, consider extending your CIF authorisation or applying for a CASP authorisation under Article 62 of MiCAR.

MiCAR service	Equivalent MiFID investment service / activity
Providing custody and administration of crypto-assets on behalf of clients	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 crypto-assets	Operation of a multilateral trading facility or operation of an organised trading facility (as applicable)
Exchange of crypto-assets for funds and other crypto assets	Dealing on own account
Execution of orders for crypto-assets on behalf of clients	Execution of orders on behalf of clients
Placing of crypto-assets	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 crypto-assets on behalf of clients	Reception and transmission of orders in relation to one or more financial instruments
Providing advice on crypto-assets	Investment advice
Providing portfolio management on crypto-assets	Portfolio management
Providing transfer services for crypto-assets on behalf of clients	No equivalent MiFID service or activity



2. How do I notify CySEC?

How to submit:

- Complete CySEC [Form 1-MiCAR](#) (notification under Article 60 of MiCAR). Part D of the form requires, among other things, your organisational and group structure (if applicable), an updated internal operations manual including policies relevant to your intended crypto-asset services, and the core information listed below.
- The applicable fee is outlined in [Directive DI 73-2009-04](#)

❖ CySEC may request clarifications during its review.

What to include in your notification:

Core information (required for all firms):

- Program of operations: A three-year business plan detailing your structure, services, target markets, client types, resources, outsourcing arrangements, and financial projections.
- AML/CFT framework: Controls for anti-money laundering and counter-terrorist financing, including due diligence, reporting procedures, and staff training.
- Business continuity plans: Measures for service continuity, testing protocols, third-party contingencies, and key-person risk management.
- ICT systems & security: Overview of technology infrastructure, cybersecurity measures, risk management, and DORA compliance. Include both technical documentation and a non-technical explanation.
- Asset segregation: How clients' crypto-assets and funds are kept separate from the firm's own, including wallet segregation, safeguarding of keys, and deposit arrangements with credit institutions.
- Crypto-asset types: Specify whether you intend to offer ARTs, EMTs, or other crypto-assets.

Service-specific information (as applicable):

- Custody/administration: Setup, risk controls, key management, outsourcing oversight, and procedures for asset return/loss.
- Trading platform: Admission and trading rules, execution and settlement processes, fee structures, and market abuse prevention.
- Exchange services: Non-discriminatory commercial policy and pricing methodology, accounting for volume and market volatility.
- Order execution: Venue selection, best execution criteria, client consent, order monitoring, and policy disclosure.
- Advisory/portfolio management: Staff expertise, internal policies, and ongoing training requirements.
- Transfer services: Asset types, risk management, ICT arrangements, insurance coverage, and client information procedures.
- ❖ If any of the above information has already been submitted to CySEC, you may simply confirm that it remains up to date.

3. How long does the notification process take?

Notification process for CySEC

- Firms must submit their notification at least 40 working days before starting crypto-asset services.
- CySEC will assess the submission for completeness within 20 working days. If documentation is missing or incomplete, CySEC will request the outstanding materials, which must be submitted within 20 working days, extending the review period.
- The maximum processing time is 60 working days, provided all documentation is complete.

⚠ Firms may not begin offering crypto-asset services until CySEC confirms the notification is complete.

Once confirmed, the firm will be listed in ESMA's public register of CASPs.

❖ Submit comprehensive documentation upfront to avoid delays.



4. What are the obligations ?

MiCAR is largely aligned with MiFID II, so most requirements will be familiar to CIFs.

Prudential requirements:

No additional capital is required if your CIF licence covers equivalent services. You continue to follow existing CIF and IFD capital and prudential requirements.

What you need to update:

MiCAR introduces additional obligations in the following areas:

- Governance – Employees and managers must demonstrate appropriate skills and knowledge (see grey box below).
- Policies & procedures – Update to reflect MiCAR-service-specific obligations (see Q.2)
- Business continuity – Align accordingly with the Digital Operational Resilience Act (DORA)
- Client communications – Update disclosures and complaints handling; include environmental impact disclosures for crypto-asset activities.
- Market abuse – Update policies to reflect MiCAR's market abuse regime (similar to MAR) and train staff accordingly.

CIFs are well-positioned for MiCAR compliance through targeted updates to policies, governance, systems, and

staff training on crypto-specific risks.

Note: If your firm reaches 15 million active EU users annually, you will be classified as a Significant CASP, triggering additional reporting obligations to CySEC and ESMA.

5. Can I passport crypto-asset services across the EU?

Yes. CIFs can offer crypto-asset services throughout the EU under MiCAR's passporting regime.

How to passport:

Notify CySEC with the following details:

- Member States where services will be offered
- Specific crypto-asset services to be provided on a cross-border basis
- Planned start date
- Any other activities provided that fall outside MiCAR

Timeline:

- CySEC will forward your notification to host Member States, ESMA, and EBA within 10 working days.
- You may begin offering services once CySEC confirms the notification has been sent, or 15 calendar days after submission, whichever comes first.

ESMA issued [final guidelines](#) setting EU-wide standards for staff competence covering two categories:

1. Information providers must understand crypto-asset characteristics, risks, DLT functionality, costs (including gas fees), market dynamics, and regulatory protections.

Minimum requirement: 80 hours of training + 6 months supervised experience, or 1 year experience.

2. Advisors require all of the above plus expertise in suitability assessments, portfolio diversification, valuation methods, and Article 81 of MiCAR obligations.

Minimum requirement: A degree + 1 year experience, or 160 hours training + 1 year experience.

Ongoing obligations:

- Annual CPD (Continuing Professional Development) covering regulatory, market, and technology updates.
- Staff must understand crypto-specific risks: volatility, cybersecurity, private key management, DLT interoperability, and operational risks.



❖ Key difference: MiCAR Vs. MiFID II

- ❑ **No client categorisation** under MiCAR (e.g., retail/professional distinctions do not apply).
- ❑ **No appropriateness test** required for crypto-asset services.
- ❑ **Environmental disclosures** are mandatory for consensus mechanisms under MiCAR, but firms are not required to collect clients' sustainability preferences.
- ❑ MiCAR introduces a separate **market abuse regime** tailored to crypto-assets.
- ❑ **No product governance obligations** under MiCAR (e.g., target market definition, distribution strategy).
- ❑ **Staff competence across the value chain**, MiCAR requires verifiable, crypto-specific knowledge across roles, not just client-facing. Staff must understand DLT, asset risks, cost structures, and investor protection differences.

⚠ Note: While some MiFID II protections do not apply under MiCAR, CIFs must still ensure strong client protection through clear disclosures, effective complaints handling, and robust conflict-of-interest management

How can KPMG support your MiCAR transition ?

- ❑ **MiCAR readiness & notifications:** We help you assess your current framework against MiCAR requirements, identify compliance gaps, and prepare comprehensive notifications to CySEC to ensure timely approval and EU-wide passporting.
- ❑ **Compliance updates:** Our team supports the update of internal policies and procedures to reflect MiCAR-specific obligations.
- ❑ **Governance & risk management:** We assist in aligning your governance and risk frameworks with MiCAR standards by enhancing management body oversight; implementing staff competence frameworks (per ESMA guidelines); updating risk assessment methodologies, while leveraging your existing CIF controls.
- ❑ **Operational & technical solutions:** We guide the implementation of systems and controls to meet MiCAR and DORA requirements, including crypto-asset custody and segregation of client assets; ICT security arrangements; operational resilience and continuity planning.

Contact us

Marios Lazarou

Board Member, Head of Advisory
T: +357 22 209 107
E: Marios.Lazarou@kpmg.com.cy

Eleni Poyiadji

Principal, MiFID expert
T: +357 22 209 248
E: Eleni.Poyiadji@kpmg.com.cy

Marie-Hélène Angelides

Senior Associate, Regulatory Compliance
T: +357 22 209 227
E: mangelides@kpmg.com

kpmg.com.cy



©2025 Limited, a Cyprus limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.