WHITEPAPER

MARKETS IN CRYPTO-ASSETS REGULATION (MICAR)

MICAR – EUROPE'S BRIDGE TO THE CRYPTO FUTURE OR A REGULATORY WALL?

Foto: Getty Images

AUTHORS:
NIKOLAI KÖNIG, MORITZ REINDL

protiviti®
Global Business Consulting

CONTENTS

LIST OF FIGURES

1. EXECUTIVE SUMMARY

The Markets in Crypto-Assets Regulation (MiCAR) represents a fundamental shift in how crypto-asset markets are governed in the European Union. Rather than introducing incremental compliance requirements, MiCAR effectively forces crypto-native business models to align with bank-grade expectations for governance, risk management, operational resilience, transparency, and auditability.

For Issuers and Crypto-Asset Service Providers (CASPs), MiCAR is not simply a legal hurdle. It reshapes the target operating model across five critical dimensions:

- **Governance & Accountability:** Formalized management responsibility, fit-and-proper requirements, and conflict-of-interest frameworks.
- **Technology & ICT Resilience:** Stronger expectations for secure, resilient, and well-controlled IT environments, closely aligned with DORA.
- **Data & Transparency:** Enhanced disclosure, transaction traceability, and data lineage obligations, including Travel Rule compliance.
- **Controls & Risk Management:** Market abuse surveillance, suitability assessments, capital and liquidity controls, and business continuity.
- **Auditability & Supervisory Readiness:** Increased supervisory intensity, on-site inspections, and the need for demonstrable, testable control frameworks.

MiCAR creates a strategic fork in the road. Firms that treat MiCAR as a transformation program can leverage regulatory clarity to scale across the EU single market, build institutional trust, and differentiate through strong governance and controls. Firms that approach MiCAR as a narrow compliance exercise risk higher costs, delayed market entry, and supervisory friction which acts as a permanent drag on innovation and erodes the agility needed to compete in a rapidly evolving digital asset landscape.

Whether MiCAR becomes a bridge to sustainable growth or a regulatory wall that redirects innovation will depend on how effectively organizations integrate regulatory requirements into their operating models, technology architectures, and internal control frameworks.

2. WHY MICAR? FROM MARKET VOLATILITY TO SUPERVISORY ARCHITECTURE

Since the launch of Bitcoin in 2009, Crypto-Assets have evolved from a niche innovation into a global financial phenomenon. Alongside innovation, the market has been characterized by extreme volatility, fragmented regulation, and significant risks related to consumer protection, market integrity, and financial crime.

Prior to MiCAR, the EU regulatory framework applied only partially to Crypto-Assets, primarily where tokens qualified as financial instruments under MiFID II. This resulted in:

- Fragmented national approaches
- Regulatory arbitrage
- Limited supervisory visibility
- Inconsistent consumer protection standards

MiCAR reflects a strategic regulatory pivot. The EU has chosen to move from innovation-first to risk-first regulation, embedding Crypto-Assets into a structured supervisory architecture comparable to traditional financial markets.

MiCAR was introduced as part of the EU Digital Finance Package alongside:

- The Digital Operational Resilience Act (DORA)
- The Transfer of Funds Regulation (TFR)
- The DLT Pilot Regime

Together, these initiatives form a new regulatory control stack for digital finance. MiCAR focuses on market conduct, prudential requirements, and disclosure. DORA addresses ICT resilience. TFR operationalizes AML and Travel Rule requirements for crypto transfers. The combined effect is a step-change in supervisory expectations.

MiCAR compliance requires more than policy updates. Leading organizations treat MiCAR as a transformation of their governance, risk, and control architecture. Key strategic actions include conducting enterprise-wide MiCAR gap assessments, redesigning governance and accountability models, embedding regulatory requirements into product and IT lifecycles, aligning MiCAR and DORA implementation programs or establishing supervisory engagement models.

Firms that integrate MiCAR into their operating model can achieve faster regulatory approvals, stronger institutional credibility, and scalable EU-wide operations.

3. SCOPE AND CLASSIFICATION – WHAT REALLY FALLS IN (AND WHAT DOESN'T)

The impact of MiCAR is essentially determined by a structured regulatory classification of the respective crypto-asset. The logic follows a clear exclusion and classification principle: first, it is examined whether an asset falls within the scope of application at all, before the specific token category is then determined.

The first step is to ask the fundamental question of whether it is actually a crypto-asset within the meaning of MiCAR. A crypto-asset is a digital representation of a value or right that can be electronically transferred and stored using distributed ledger technology (DLT). Classic cryptocurrencies, stablecoins, or tokenized rights typically meet this definition. Purely digital data without transferable value, on the other hand, does not. The next step is a central distinction test against existing EU financial market regulations, as MiCAR was explicitly designed to fill gaps. It applies primarily where no harmonized EU regulations existed previously.

It is particularly important to check whether a token can already be classified as a financial instrument under MiFID II. Security tokens that represent, for example, shares, bonds, or derivatives, generally fall under MiFID II – and not under MiCAR. The same applies to certain electronic payment instruments: if a token is structured as classic e-money within the meaning of the E-Money Directive (EMD2), the provisions therein primarily apply. However, it should be noted that although so-called e-money tokens (EMTs) are closely based on e-money regulation, they are explicitly regulated by MiCAR. This does not result in complete exclusion, but rather a hybrid regulatory approach with bank-like requirements.

Another important distinction concerns deposits, structured products, and insurance products – these also remain outside the scope of MiCAR if they are already regulated by existing financial market regulations.

Only if no such exclusion applies is the asset classified within the MiCAR system. The regulation distinguishes between three main categories of tokens:

- **Asset-referenced tokens (ARTs)** are designed to maintain their value by referencing multiple assets, such as a basket of currencies or commodities. Due to potential risks to financial stability, they are subject to particularly strict requirements in terms of governance, reserve management, and risk controls. Examples for ARTs are Paxos Gold (PAXG) or tokenized resource or index tokens.
- **E-money tokens (EMTs)** pursue a narrower stability promise: their value is linked to exactly one official fiat currency. In regulatory terms, they are very similar to traditional payment instruments, which is why issuers often need to have a banking or e-money license. Examples for EMTs are USDT (Tether), USDC (USD Coin) or EURC (Euro Coin von Circle).
- All other tokens generally fall under the category of **utility tokens**, provided they grant access to a digital application or network and do not have a primary investment character. Although they are subject to less stringent requirements, they are subject to clear transparency requirements via a Crypto-Asset whitepaper. Examples for utility tokens are Filecoin (FIL), Basic Attention Token (BAT) or Chainlink (LINK).

NFTs (non-fungible tokens) represent a frequently discussed gray area. In principle, genuine, unique NFTs are exempt from MiCAR. However, the actual economic structure is decisive: if NFTs are issued in large series or are effectively interchangeable ("fractionalized" or highly standardized), supervisory authorities may interpret them as fungible tokens – which would mean they would fall within the scope of MiCAR after all. In this case, the economic reality takes precedence over the technical designation.

In summary, the determination of MiCAR applicability follows a clear regulatory logic:

1. **Is the object a transferable Crypto-Asset?**
2. **Does another EU financial market regulation already apply?** If so, this takes precedence.
3. **If not, to which token category does the asset belong?** This determines the specific regulatory requirements.

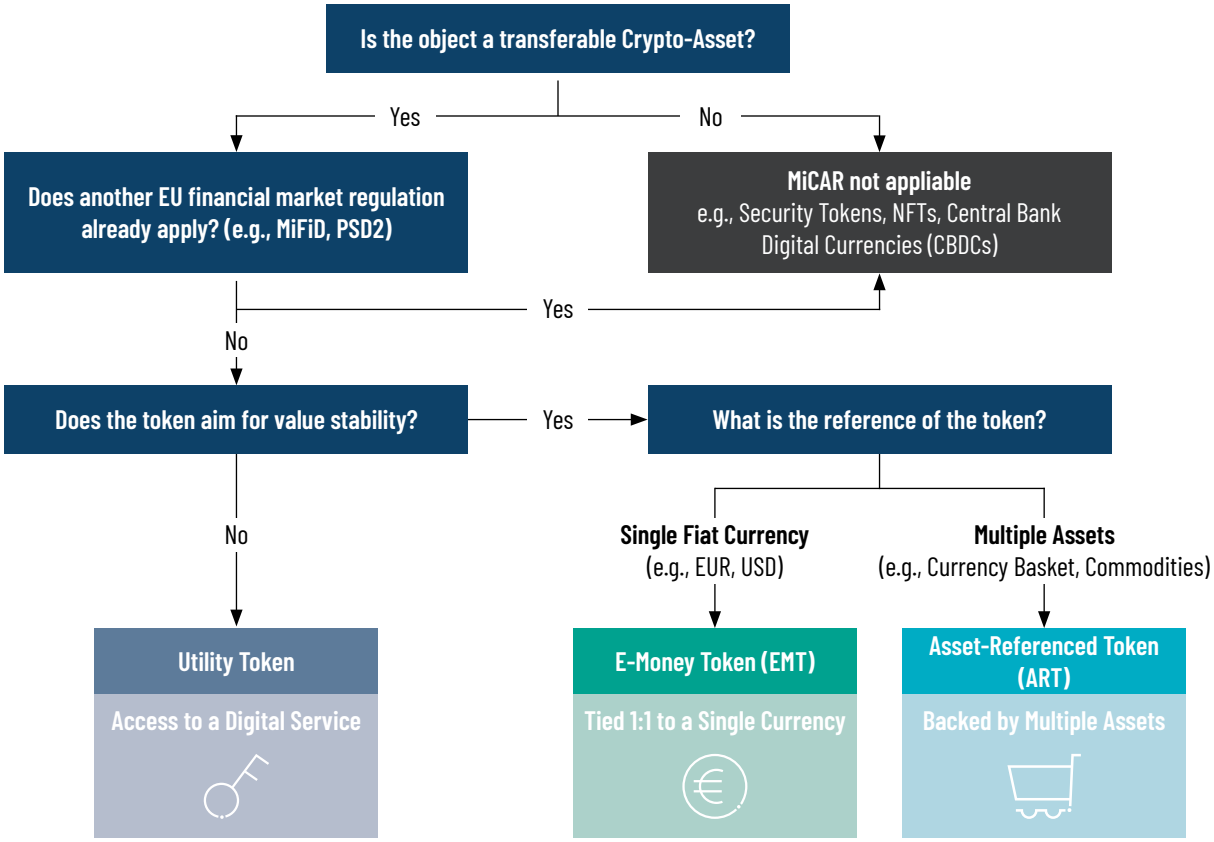

Figure 1 – Crypto-Asset MiCAR Applicability Decision Tree

For companies, this system means one thing above all: the greatest regulatory risk lies not so much in clearly regulated tokens as in **misclassification**. Incorrect classification can lead to significant compliance risks – from sales bans to regulatory measures.

From a strategic perspective, it is therefore advisable to conduct an early **regulatory product analysis**, ideally as early as the design phase of a token. Organizations should take an interdisciplinary approach and consider legal, technological, and control-related issues together. This is because MiCAR not only regulates the asset itself, but also indirectly regulates the entire operating model, including governance, risk management, and internal control systems.

Against this classification backdrop, a second – often underestimated – dimension becomes relevant: **regulatory intensity does not stop at categorization. It scales.**

While the previous section clarified whether and **under which** category a crypto-asset falls within MiCAR, the next analytical step concerns **how deeply** the regulation penetrates the operating model of the issuing or servicing entity.

MiCAR does not apply in a uniform manner across all token types or market participants. Instead, it operates along a **control gradient**: the breadth and depth of governance, safeguarding, and supervisory expectations increase in proportion to the economic function, risk profile, and systemic relevance of the respective activity.

At the lower end of this gradient are utility-oriented token models with limited financial risk exposure and comparatively moderate regulatory obligations. Moving upward, regulatory intensity increases significantly – particularly for Asset-Referenced Token (ART) issuers, E-Money Token (EMT) issuers, and licensed Crypto-Asset Service Providers (CASPs).

This escalation is primarily driven by three core risk dimensions:

- Exposure to client assets and custody risk
- Market integrity and investor protection risk
- Operational and systemic relevance

The more an entity performs functions comparable to traditional financial intermediaries – such as reserve management, payment functionality, custody, or trading venue operation – the closer it moves toward institutional-grade regulatory expectations.

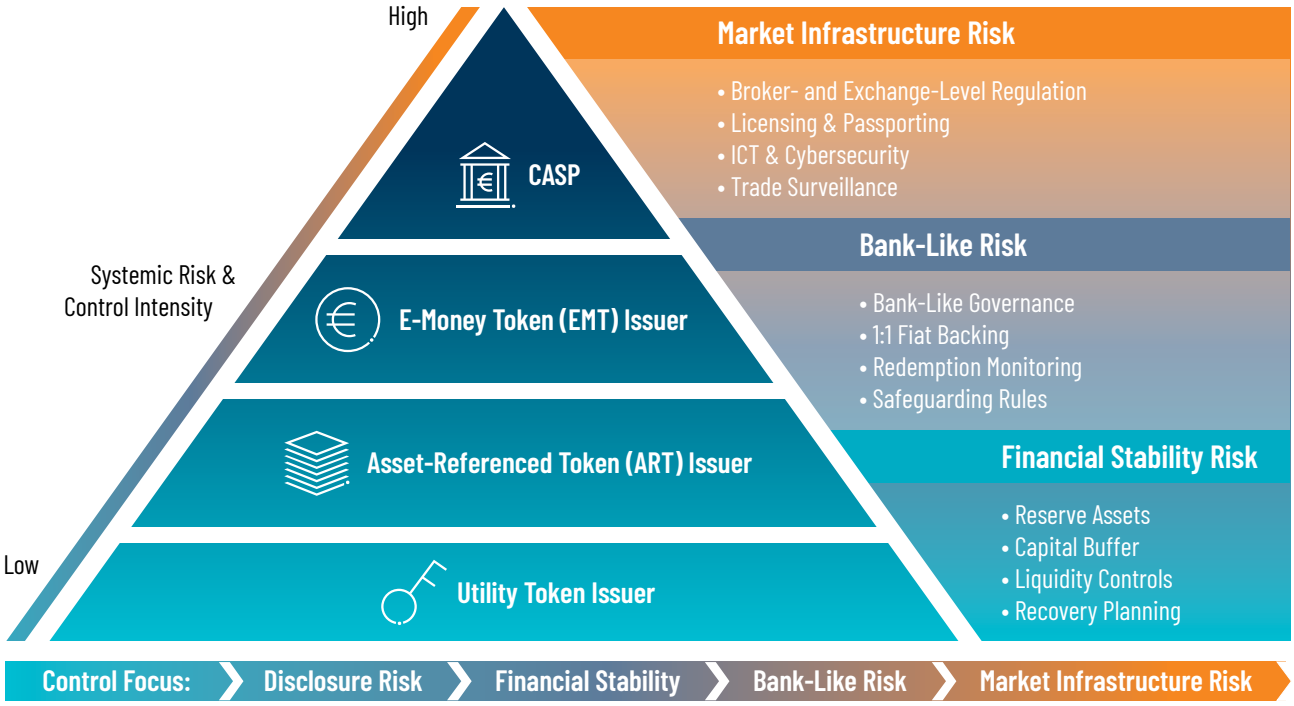

Figure 2 – MiCAR Control Gradient

In this sense, MiCAR does not regulate "technology", but rather **financial functionality executed through technology**. Regulatory intensity follows economic substance, not technical labeling. Understanding this control gradient is essential for translating token classification into concrete implementation requirements. The following chapters therefore examine the specific obligations for token issuers and Crypto-Asset Service Providers in greater detail, outlining how MiCAR's proportionality principle materializes in governance structures, safeguarding mechanisms, risk management frameworks, and internal control systems.

4. ISSUERS – FROM WHITEPAPER TO ONGOING SUPERVISION

Under MiCAR, issuers represent the regulatory entry point for Crypto-Assets into the EU market. The framework fundamentally shifts their role from technical token creators to regulated product sponsors with ongoing supervisory accountability.

Issuance is no longer a purely technical or entrepreneurial act. It becomes a regulated market activity embedded within a formal governance and control environment.

4.1 Issuers as Regulated Product Sponsors

MiCAR effectively positions issuers as operating model owners responsible for the full lifecycle of their Crypto-Asset. This includes:

- Product governance and risk assessment
- Transparent and accurate market disclosure
- Conflict-of-interest management
- Complaint-handling mechanisms
- Financial and operational resilience

The degree of regulatory intensity depends on the token category. While utility token issuers face primarily disclosure-based requirements, issuers of Asset-Referenced Tokens and E-Money Tokens are subject to significantly enhanced prudential, governance, and reserve management obligations.

Irrespective of category, MiCAR establishes a clear supervisory expectation: Issuers must be able to demonstrate that their organizational structures, controls, and governance arrangements are proportionate to the risks generated by the token model.

4.2 The Whitepaper as a Regulated Control Instrument

A central pillar of the issuer regime is the MiCAR whitepaper.

It is no longer a marketing document, but a legally relevant disclosure instrument subject to regulatory review and liability standards. Its purpose is to

provide investors with clear, fair, and not misleading information regarding:
- Token characteristics and rights
- Underlying technology
- Risks and dependencies
- Governance structures
- Issuer identity and accountability

Importantly, the whitepaper is not static. Material changes to the business model, token economics, reserve structures, or risk profile may trigger update obligations.

From a governance perspective, this transforms the whitepaper into a controlled regulatory artifact that must be embedded within formal product lifecycle management processes. Version control, approval workflows, and monitoring mechanisms become essential.

4.3 Core Regulatory Requirements

In practical terms, issuers must:
- Be legally established within the EU and, where required, authorized by the relevant national competent authority (e.g. BaFin for Germany)
- Prepare and publish a MiCAR-compliant whitepaper for each Crypto-Asset
- Implement robust conflict-of-interest and complaints procedures
- Maintain appropriate capital or reserve arrangements (particularly for ARTs and EMTs)
- Establish secure ICT systems and business continuity frameworks

These requirements extend beyond legal compliance. They require operationalization through documented policies, clearly assigned responsibilities, and effective internal controls.

4.4 Controls Perspective

From a technology audit standpoint, the critical implementation challenge lies in integration. Regulatory disclosures must be aligned with DORA requirements amongst others, concerning e.g.,
- Risk management processes
- ICT and security controls
- Incident and change management
- Ongoing monitoring of token performance and market behavior

Failure to treat the whitepaper and associated governance obligations as controlled elements of the operating model increases supervisory, liability, and reputational risk.

MiCAR therefore transforms issuance from a launch event into a continuously supervised activity – one that requires institutional-grade governance from day one.

5. CASPS – CRYPTO FIRMS WITH BANK-GRADE CONTROLS

MiCAR fundamentally repositions CASPs closer to traditional regulated financial institutions. Authorization is no longer a market access formality, it becomes a comprehensive assessment of governance, controls, and operational readiness.

» Not all CASPs are created equal, thus MiCAR requirements depend on the kind of Crypto-Asset services provided by the CASP and the associated systemic risk.«

NIKOLAI KÖNIG
DIRECTOR IAFA-TECH AUDIT & ADVISORY

5.1 CASPs from a Control Framework Perspective

MiCAR requires CASPs to design and operate control environments across the following domains. The control requirements that a CASP must meet depend on the category of Crypto-Asset services it provides, whereby the requirements of the domains 'Governance and Fit-and-Proper' and 'Technology and ICT Controls' must be met by every CASP regardless of this:

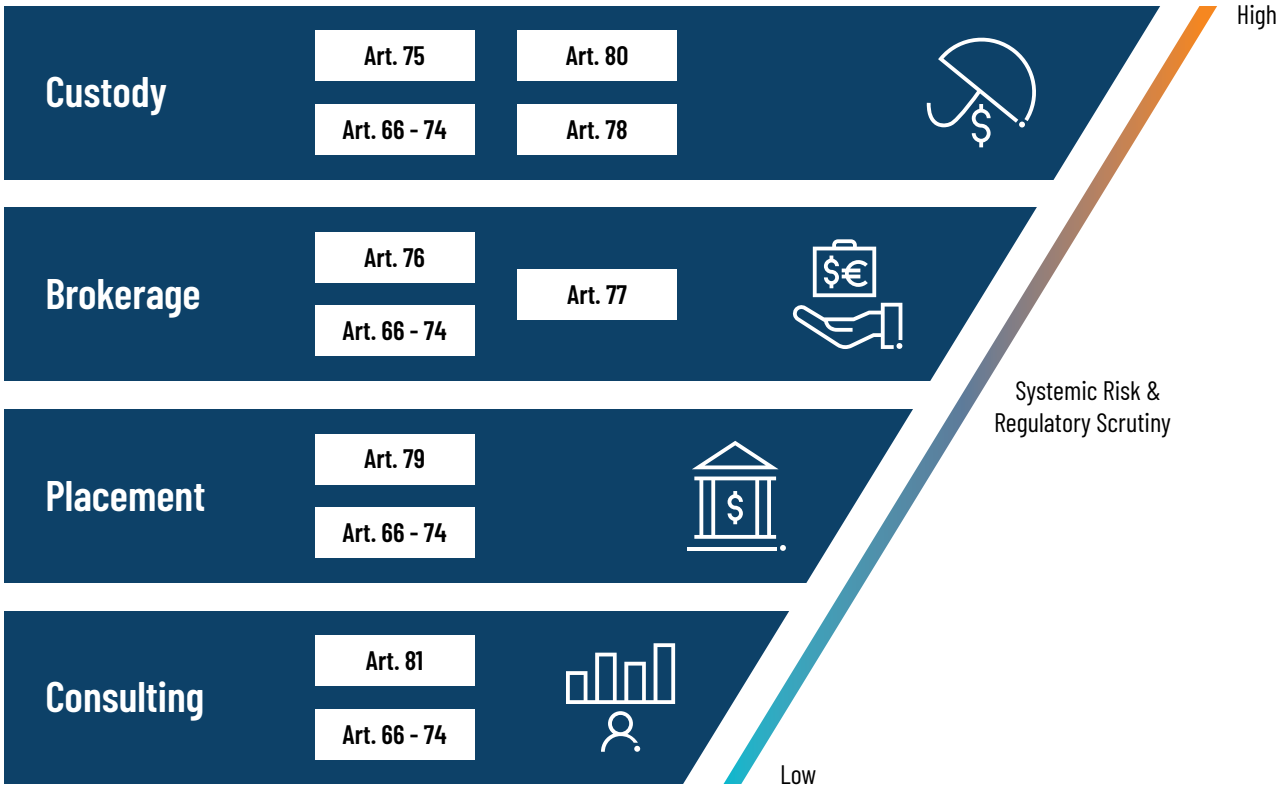

Figure 3: CASP Service Offering Control Gradient and corresponding MiCAR Articles

- **Governance and Fit-and-Proper** CASPs are required to establish a sound and accountable management framework. It must ensure that senior leadership and key function holders meet strict "fit and proper" requirements, demonstrating integrity, expertise, and the ability to oversee a regulated Crypto-Asset business effectively. It should also emphasize clear organizational structures, defined responsibilities, and robust conflict of interest management to safeguard decision making and maintain regulatory trust.
- **Technology and ICT Controls** This control domain concentrates on building a resilient, secure and well controlled technology environment. CASPs must ensure the implementation of secure system architectures, access governance, and ICT risk management processes aligned with EU wide operational resilience standards (DORA). The objective is to ensure service continuity, prevent cyber incidents, protect client assets, and maintain trustworthy and secure operations across all technology layers.
- **Market Integrity and Conduct** CASPs need to demonstrate that they operate fairly, transparently, and free from abusive practices. CASPs are required to establish mechanisms to detect and prevent market manipulation, insider dealing, and other forms of misconduct, especially for trading venues and brokerage activities. The focus is on maintaining transparent pricing, robust trade surveillance, and reliable pre and post trade information to uphold confidence in Crypto-Asset markets.
- **Client Protection and Suitability** CASPs are required to safeguard clients by ensuring that services, products, and information are appropriate for their knowledge level and risk tolerance. This control domain includes clear client classification, suitability assessments where required, and transparent disclosure of all material risks. The aim is to protect retail and institutional clients alike and ensure that CASPs engage in fair, clear, and non-misleading communication.
- **Data, AML and Travel Rule Compliance** CASPs must ensure the integrity, accuracy, and traceability of client and transactional data. This control domain ensures that CASPs comply with stringent EU AML and Travel Rule requirements, including the transmission of verified originator and beneficiary information across counterparties. The focus is on robust KYC data standards, end-to-end traceability of Crypto-Asset transfers, and interoperability with other service providers to prevent financial crime and enhance regulatory transparency.

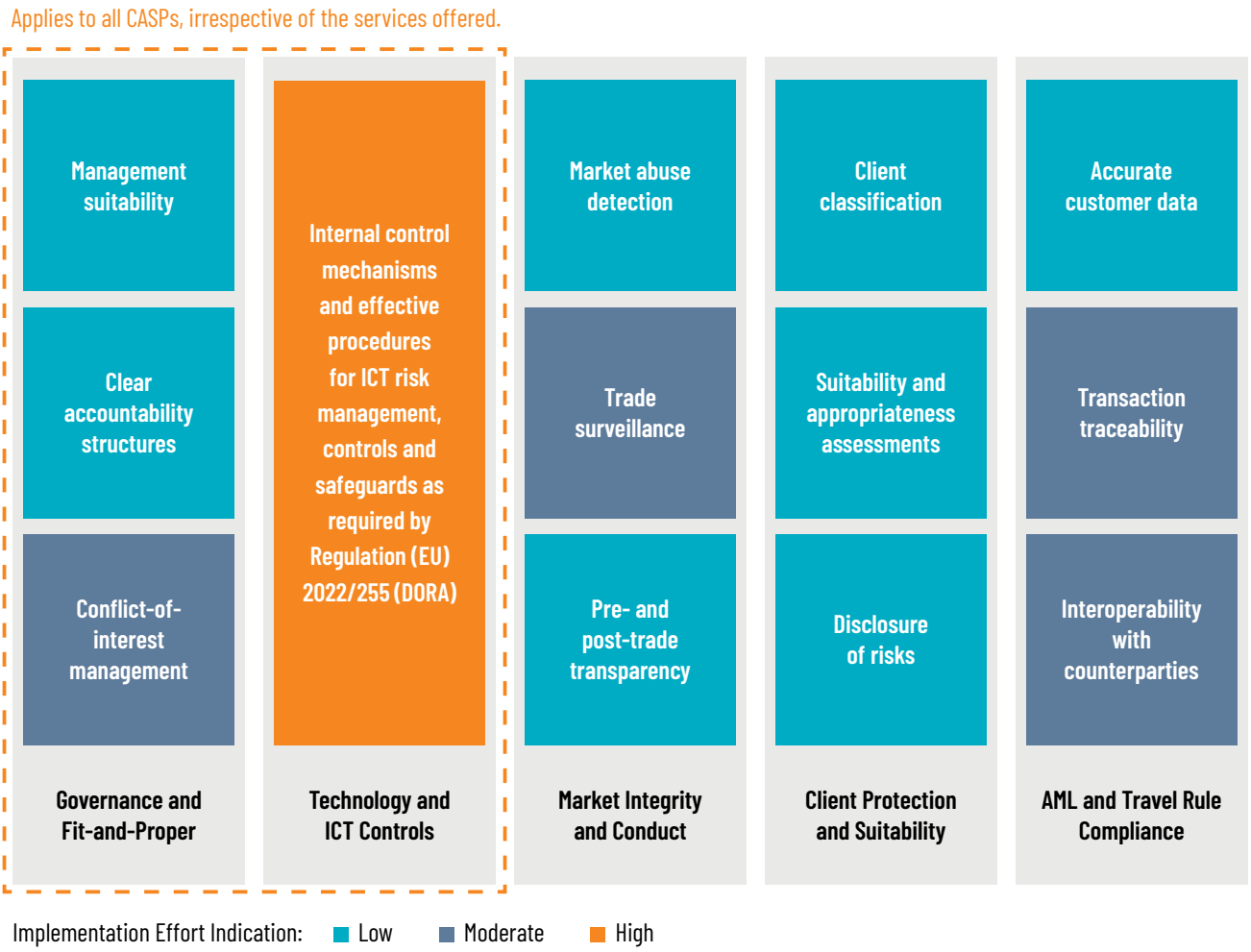

Figure 4: CASP Control Domain Heatmap evaluated by implementation effort

For many CASPs, MiCAR is the first time their control environment will be assessed against standards comparable to regulated banks and investment firms. While Governance and Fit and Proper requirements are generally less burdensome – given their procedural and organizational nature – Technology and ICT Controls stand out as the most demanding domain due to MiCAR's integration with DORA, the need for robust ICT risk management, and the operational complexity of securing distributed ledger-based infrastructures.

Market Integrity and Conduct requirements fall into a medium effort category, as they require sophisticated surveillance capabilities and transparent market conduct procedures, but only for CASPs offering trading or exchange related services.

Client Protection and Suitability, by contrast, tend to be less resource intensive and mainly require standardized disclosure, classification, and appropriateness processes.

Data, AML, and Travel Rule Compliance also impose a medium level of effort, as CASPs must ensure high quality customer data, transaction traceability, and interoperability with counterparties, but these efforts are largely process driven rather than structurally transformative.

6. MICAR, DORA AND TFR – THE EMERGING DIGITAL CONTROL STACK

MiCAR must not be viewed in isolation. Its implementation unfolds within a broader EU regulatory architecture that collectively reshapes digital finance:

- **MiCAR:** market conduct, governance and prudential safeguards
- **DORA:** ICT risk management and operational resilience
- **TFR:** AML transparency and Travel Rule data flows

Together, these regimes form a new digital control stack. MiCAR governs the business model, DORA the technological resilience, and TFR the transparency of crypto transfers. Importantly, MiCAR relevance does not automatically trigger DORA applicability. DORA applies to entities that qualify as financial institutions under its own scope provisions. In practice, most licensed Crypto-Asset Service Providers (CASPs), ART and EMT issuers will fall within DORA, while certain utility token issuers may not.

Nevertheless, even where DORA does not formally apply, MiCAR introduces governance, safeguarding and ICT-related obligations that converge with operational resilience standards.

For firms, the core challenge is therefore architectural rather than interpretative. Controls must be designed holistically to ensure end-to-end data lineage, secure Travel Rule integration, robust ICT resilience, and auditability across on- and off-chain environments.

Organizations that approach MiCAR, DORA and TFR as an integrated framework – rather than separate compliance projects – will reduce redundancy, strengthen supervisory readiness, and position themselves as institution-grade market participants.

7. INTERNAL AUDIT AND ON-CHAIN ANALYTICS – A NEW ASSURANCE MODEL

MiCAR fundamentally reshapes the supervisory landscape for crypto-asset markets. Regulatory authorities are granted far-reaching powers, including on-site inspections, thematic reviews, data requests, and ad hoc investigations. This shift signals a clear expectation: crypto firms must transition from startup-style governance toward institutional-grade control environments.

Within this evolving framework, internal audit is no longer merely a retrospective control function – it becomes a strategic enabler of regulatory readiness and operational resilience.

Supervisors will increasingly assess not only whether controls exist, but whether firms can demonstrate control effectiveness through reliable, traceable, and independently verifiable data. This is precisely where blockchain-native transparency introduces a structural transformation to the assurance model.

7.1 From Periodic Audits to Continuous Assurance

Traditional internal audit approaches rely heavily on sampling, ex-post testing, and management-provided documentation. While these methods remain relevant, they are inherently limited in environments characterized by high transaction velocity, algorithmic execution, and near real-time asset transfers.

Blockchain technology challenges this paradigm. Because many crypto transactions are recorded on public or permissioned ledgers, auditors gain access to an immutable and time-stamped data layer that can be independently validated. When systematically leveraged, this data enables a transition from periodic assurance toward continuous, data-driven oversight.

This evolution mirrors developments already observed in highly regulated capital market infrastructures, where supervisors increasingly expect near real-time risk visibility.

7.2 On-Chain Analytics as Audit Evidence

On-chain analytics allows internal audit functions to analyze blockchain-native data without relying solely on management representations. Key areas of review may include:

- Token issuance mechanics and circulating supply
- Treasury wallet activity and reserve movements
- Transaction flows and concentration risks
- Smart contract execution patterns
- Related-party interactions
- Liquidity signals across trading venues

For internal audit, this creates a fundamentally stronger evidentiary basis as on-chain data is:

- **Immutable**, reducing the risk of post hoc manipulation
- **Independently verifiable**, strengthening audit defensibility
- **Highly granular**, enabling deeper forensic analysis
- **Near real-time**, allowing earlier risk identification

The result is not simply better audit testing – it is a structural increase in assurance quality.

7.3 Strategic Value for Regulatory Engagement

From a supervisory perspective, firms capable of producing blockchain-based audit insights signal a higher level of operational maturity. The ability to proactively detect anomalies, reconstruct transaction histories, and substantiate reserve positions can materially improve the quality of regulatory dialogue.

Conversely, organizations that lack the tooling or expertise to interpret their own on-chain footprint may face heightened supervisory scrutiny.

In this context, on-chain analytics evolves from a technical capability into a strategic trust mechanism between firms and regulators.

8. BRIDGE OR BARRIER – THE STRATEGIC VERDICT

MiCAR is both Europe's strongest regulatory foundation for Crypto-Assets and a significant structural challenge for market participants.

Whether MiCAR becomes a bridge or a wall depends on execution: consistent supervision, pragmatic interpretation, and the ability of firms to embed regulation into scalable operating models.

Organizations that act early can turn regulatory change into a strategic advantage by proactively strengthening their operating model, ICT resilience, and control frameworks. Those that delay risk higher compliance costs, increased supervisory scrutiny, and reduced strategic flexibility.

Now is the time to move beyond compliance and redesign your organization for a regulated digital asset environment.

Start your MiCAR readiness journey today:

- Assess your MiCAR, DORA and TFR exposure and regulatory scope
- Identify gaps across governance, technology, data and controls
- Define a target operating model aligned with supervisory expectations
- Build supervisory readiness, auditability and operational resilience
- Embed MiCAR into a scalable, EU-wide growth strategy

Protiviti supports Issuers and CASPs across the full MiCAR lifecycle – from regulatory impact assessments and operating model design to ICT risk management, DORA alignment, Travel Rule readiness, and internal audit with on-chain analytics.

Turn MiCAR into a strategic advantage. Start with a structured MiCAR readiness and control maturity assessment.

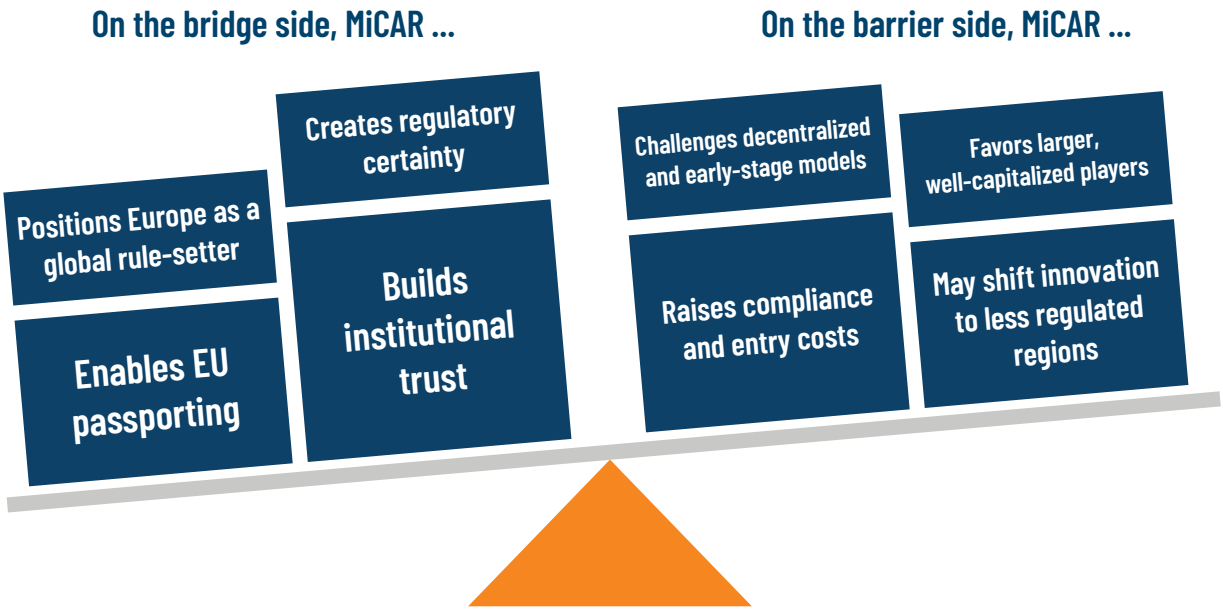

Figure 5: MiCAR: Opportunities and Challenges for the European Crypto Market

ABOUT PROTIVITI

Protiviti *(www.protiviti.com)* is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit – enabling organizations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the **Fortune 100 Best Companies to Work For®** list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of **Robert Half** (NYSE: RHI).

In the context of MiCAR, Protiviti supports Issuers and CASPs across the full lifecycle, from regulatory strategy and operating model design to technology controls, internal audit, and supervisory readiness.

www.protiviti.de

CONTACT

NIKOLAI KÖNIG
Director
+49 172 698 3047
nikolai.koenig@protiviti.com

ANDREJ GREINDL
Managing Director
+49 172 698 30 53
andrej.greindl@protiviti.com