OLEKSANDR POTAPENKO
FINTECH ARCHITECT
FOUNDER

The MiCA Survival Guide: Navigating the EU's New Regulatory 'Great Filter'

GUIDE FOR APPLICANTS | OCTOBER 2025

This report provides a strategic overview of the MiCA licensing landscape, key regulatory challenges, and the critical role of technology in a successful application. Data is based on public market analysis and insights from recent regulatory deficiency letters.

---

1. The New Landscape: A 'Great Filter'

The Markets in Crypto-Assets (MiCA) regulation has replaced Europe's fragmented national crypto regimes with a single, high-barrier "gatekeeper" model. The era of "regulatory arbitrage"—seeking easy licenses in certain jurisdictions—is over.

Regulators are now actively filtering the market, and the initial data shows a massive consolidation.

By the Numbers (2024-2025):

- **Massive Consolidation:** The number of active Virtual Asset Service Providers (VASPs) in the EU peaked at over 3,100 before MiCA's implementation.
- **Low Approval Volume:** As of mid-2025, only **53 total MiCA licenses** have been granted across the EU (39 CASPs and 14 EMT issuers). Projections estimate only 110-130 licensed CASPs by the end of 2025.
- **A "Flight to Quality":** Applicants are no longer choosing jurisdictions based on ease. The licenses are heavily concentrated in high-scrutiny member states, with **Germany (12) and the Netherlands (11)** alone accounting for over 43% of all initial approvals.

The clear takeaway is that regulators are not "processing" applications; they are **filtering** them. Success rates are low not just from outright rejections, but because a significant number of applicants withdraw when faced with exhaustive questions they cannot answer.

OLEKSANDR POTAPENKO
FINTECH ARCHITECT
FOUNDER

2. Why Applications Fail: The Regulator's View

Analysis of market reports and regulatory deficiency letters shows that applications are being rejected for clear, predictable failures. Regulators, like Germany's BaFin, warn that incomplete or inconsistent applications will be rejected due to short statutory deadlines.

Top 4 Reasons for Failure:

1. **Inadequate AML/CFT Framework:** This is the #1 failure point. Applicants present generic, template-based AML policies that are not customized to local AML Acts, fail to properly define Politically Exposed Persons (PEPs), and cannot demonstrate a functional transaction monitoring system.
2. **Incomplete or Inconsistent Application:** The business plan, terms of service, website, and white paper are often contradictory. Regulators have found applicants claiming to partner with critical suppliers who explicitly state they are not MiCA-compliant.
3. **Weak Governance & Substance:** The management body is not deemed "fit and proper". The organizational structure is unclear, with key management scattered across jurisdictions and no clear "effective place of management."
4. **Failure to Prove Prudential Requirements:** Applicants fundamentally miscalculate their capital requirements or, more simply, **fail to provide bank statements** proving the capital is actually in the company's account.

---

3. The Core Challenge: The DORA & IT Gauntlet

Beyond governance and finance, the **Digital Operational Resilience Act (DORA)** is the new technical gauntlet. It is no longer enough to *say* you have an IT policy; you must *prove* it. Regulators are demanding a complete **ICT Risk Management Framework** from day one.

Key IT & DORA Requirements You Must Meet:

- **ICT Third-Party Risk Management:** You must provide a complete **"Register of Information"** detailing all contractual arrangements with third-party ICT providers (e.g., custodians, cloud hosts, blockchain analytics).
- **Digital Resilience Testing:** You must submit your entire resilience testing program, proving how you test your systems, including any third-party services you rely on.
- **ICT Incident Reporting:** You must have a formal process for classifying and reporting major ICT-related incidents to regulators.

- **Custody & Asset Segregation:** You must provide detailed policies for cryptographic key management, asset segregation (distinguishing client vs. firm assets), and business continuity.

For an applicant, this creates a massive technical and administrative burden. You must not only *have* these systems but also *document and audit* your relationships with every vendor you use.

---

4. How to Survive: The Integrated Vendor Advantage

In this new "filter" environment, attempting to build your own tech stack or patch together multiple standalone vendors is a high-risk strategy. It creates a fragmented, complex, and difficult-to-audit system that regulators will reject.

The only viable path is to partner with a reliable, institutional-grade vendor whose platform provides an **integrated, auditable, and pre-configured solution** to the key challenges.

Here is how a single, modern platform addresses the regulator's hardest questions:

Solves AML & The Travel Rule

The FATF Travel Rule, which MiCA incorporates, requires you to share originator and beneficiary information for transactions.

- **The Wrong Way:** Subscribing to a standalone blockchain analytics tool (like TRM Labs or Elliptic) still requires you to build your own case management, risk-scoring engine, and reporting framework.
- **The Right Way:** A platform with **native integrations** for these tools solves the problem instantly. It automates VASP screening, provides real-time transaction monitoring, and generates the auditable AML/Travel Rule reports the regulator demands. Regulated EMIs are *already* using this exact model to streamline their MiCA compliance.

Solves Custody & Asset Segregation

Regulators demand robust custody policies and proof of segregation.

- **The Wrong Way:** Relying on fragmented hardware wallets or self-developed solutions creates a documentation and security nightmare that cannot be easily audited.

- **The Right Way:** A platform built on battle-tested custody infrastructure (like **Fireblocks**) comes with these policies and procedures out-of-the-box. It provides institutional-grade key management, asset segregation, and clear workflows, allowing you to *show* the regulator your compliant custody system instead of just describing it. This is the model successful MiCA-regulated stablecoins are already using.

Solves the DORA Nightmare

DORA requires you to manage and document *all* third-party ICT risks.

- **The Wrong Way:** Using 5-10 different vendors (for custody, AML, core ledger, etc.) creates a massive contractual and oversight burden. You must prove *each one* is DORA-compliant.
- **The Right Way:** Consolidating with a **single, integrated platform** dramatically simplifies your DORA obligations. You manage one critical, well-documented vendor relationship, not ten. Your core banking, custody, and AML systems are all covered under one ICT framework, making your "Register of Information" clean, simple, and defensible.

Conclusion: A successful MiCA application is not a legal exercise; it is an **engineering and operational one**. The regulator's goal is to filter out firms that cannot demonstrate institutional-grade resilience. A technology partner with a fully integrated, pre-audited platform is no longer a luxury—it is the essential foundation for survival.