EU DIGITAL FINANCE REGULATORY FRAMEWORK

DORA & MiCA Readiness: A Practical Quick-Start Guide

Operational Resilience & Crypto-Asset Compliance in the European Union

Viktor Borisov — Compliance & Regulatory Affairs Officer • viktorborisov.com

Introduction: The Dual Regulatory Reality

The EU digital finance landscape operates under two interlocking pillars: **DORA** (Regulation (EU) 2022/2554) and **MiCA** (Regulation (EU) 2023/1114). Both regulations are fully applicable, and supervisory expectations have shifted from implementation planning to **evidence-based enforcement**.

> **Key Integration Principle:** Crypto-Asset Service Providers (CASPs) authorized under MiCA fall directly within the scope of DORA (DORA Art. 2(1)(f) & MiCA Art. 68(7)). Achieving sustainable compliance requires treating operational resilience, ICT third-party governance, and crypto-asset conduct rules as a single integrated control environment rather than isolated checklists.

Part 1: DORA Readiness (The 5 Core Pillars)

Applies to: Financial entities listed in DORA Art. 2(1), including banks, payment/e-money institutions, investment firms, insurers, and MiCA-regulated CASPs.

1. ICT Risk Management & Governance (DORA Art. 5–16; RTS (EU) 2024/1774)

- **Management Body Accountability (Art. 5):** The board must formally approve, oversee, and receive regular training on the ICT Risk Management Framework.
- **Critical Function Mapping (Art. 8):** Document all Critical or Important Functions (CIFs) and map their exact dependencies—hardware, software, data flows, and RTO/RPO targets.
- **Continuous Detection & Continuity (Art. 10–12):** Maintain centralized logging (SIEM), immutable backups, and tested Business Continuity & Disaster Recovery (BCDR) runbooks.

2. ICT Incident Classification & Reporting (DORA Art. 17–23; RTS (EU) 2024/1772 & ITS (EU) 2025/302)

- **Initial Notification / Early Warning (Art. 19(4)(a)):** Within **4 hours** of classification (and no later than **24 hours** from detection).
- **Intermediate Report (Art. 19(4)(b)):** Within **72 hours** of the initial notification.
- **Final Report (Art. 19(4)(c)):** Within **1 month** after the intermediate report, detailing root cause and remediation.
- **Action Item (Art. 18):** Pre-configure incident classification thresholds (clients affected, downtime, data loss, economic impact) into your SOC and incident playbooks.

3. Digital Operational Resilience Testing (DORA Art. 24–27)

- **Annual Baseline Testing (Art. 24–25):** Vulnerability assessments, network security reviews, gap analyses, and scenario-based testing for all critical systems.
- **Threat-Led Penetration Testing / TLPT (Art. 26–27):** Mandatory at least **every 3 years** for significant financial entities designated by competent authorities.

4. ICT Third-Party Risk Management (DORA Art. 28–44; ITS (EU) 2024/2956)

- **Register of Information (Art. 28(3)):** Maintain a structured, up-to-date register of all contractual arrangements with ICT third-party service providers, flagging those supporting CIFs.
- **Mandatory Contract Clauses (Art. 30):** Audit existing vendor contracts to ensure they include full audit/inspection rights, data storage locations, SLA targets, subcontractor controls, and documented **exit strategies (Art. 28(8))**.

5. Threat Intelligence Sharing (DORA Art. 45)

- **Actionable Intelligence (Art. 45(1)):** Establish formal mechanisms to consume, evaluate, and document cyber threat intelligence and link findings back to your risk register.

Part 2: MiCA Readiness (CASPs & Token Issuers)

Applies to: Crypto-Asset Service Providers (MiCA Title V, Art. 59–85) and issuers of ARTs (Title III), EMTs (Title IV), and other crypto-assets (Title II).

1. Authorization & EU Substance (MiCA Art. 59–64 & Art. 143)

- **Local Substance (Art. 59(2) & Art. 68(1)):** With transitional grandfathering windows (Art. 143(3)) closed across EU Member States, operating without full CASP authorization is prohibited. Entities must maintain a registered office, real management, and at least one EU-resident director in the authorizing Member State.
- **Reverse Solicitation Limits (Art. 61):** Any marketing, promotion, or communication directed at EU clients eliminates the ability to rely on “client’s own initiative” exemptions.

2. Prudential & Safeguarding Controls (MiCA Art. 67–70 & Annex IV)

- **Minimum Capital (Art. 67 & Annex IV):** Maintain permanent minimum capital (€50,000, €125,000, or €150,000 depending on service class) or one-quarter of fixed overheads from the preceding year.
- **Segregation of Client Assets (Art. 70 & Art. 75):** Strict legal and operational separation of client crypto-assets and funds from the firm’s own estate, supported by daily reconciliations and robust key-management (custody) policies.

3. Conduct, White Papers & Market Abuse (MiCA Art. 4–15, Art. 66, Art. 86–92 & TFR)

- **White Paper Compliance (Art. 6, Art. 19, Art. 51 & Art. 143(2)):** Ensure all public offers or admissions to trading are backed by compliant, ESMA-formatted white papers (noting the December 31, 2027 deadline under Art. 143(2)(b) for legacy tokens admitted prior to December 30, 2024).
- **Market Abuse Surveillance (Title VI, Art. 86–92):** Implement systems to detect and report insider dealing (Art. 89), unlawful disclosure (Art. 90), and market manipulation (Art. 91) in crypto-assets.
- **AML / Travel Rule Alignment (MiCA Art. 68(8) & Regulation (EU) 2023/1113):** Synchronize MiCA onboarding and transfer controls with EU AML obligations and Transfer of Funds Regulation (TFR Art. 14–18) originator/beneficiary data-sharing rules.

Part 3: 30-60-90 Day Readiness Checklist

Phase	Priority Actions	Key Deliverable / Evidence
Days 1–30 **Scope & Gap Analysis**	• Confirm exact regulatory scope (MiCA service classes + DORA proportionality tier). • Map Critical or Important Functions (CIFs) and supporting ICT assets. • Inventory all third-party ICT vendors.	Approved Scope Memo & ICT Asset / Dependency Map
Days 31–60 **Governance & Controls**	• Build the DORA Register of Information (Art. 28) and flag Art. 30 contract gaps. • Update Incident Response Playbooks with 4h/24h/72h reporting workflows (DORA Art. 19). • Finalize custody segregation (MiCA Art. 70/75), prudential calculations (Art. 67), and AML/TFR workflows.	DORA Register of Information & Incident Escalation SOP
Days 61–90 **Testing & Assurance**	• Execute BCDR tabletop exercises and annual resilience testing (DORA Art. 11 & Art. 24–25). • Initiate vendor contract addenda (DORA Art. 30) and document exit plans for critical providers. • Conduct an internal readiness audit (ISO 27001 / DORA / MiCA aligned).	Audit Readiness Report & Board Sign-Off Package

Key EU Legislative & Technical Standard References

1. **DORA:** Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (OJ L 333, 27.12.2022).
2. **MiCA:** Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (OJ L 150, 9.6.2023).
3. **TFR (Travel Rule):** Regulation (EU) 2023/1113 of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets (OJ L 150, 9.6.2023).

4. **DORA Level 2 Standards:** Commission Delegated Regulation (EU) 2024/1774 (ICT Risk Management), Delegated Regulation (EU) 2024/1772 (Incident Classification), Implementing Regulation (EU) 2024/2956 (Register of Information), and Implementing Regulation (EU) 2025/302 (Incident Reporting Templates).

Need a Second Pair of Eyes on Your Controls?

Building compliance frameworks that withstand regulatory scrutiny requires bridging legal obligations with technical reality.

Viktor Borisov — Compliance & Regulatory Affairs Officer | ISO 27001 Internal Auditor
Website & Free Courses: **viktorborisov.com** • LinkedIn: **linkedin.com/in/viktor-borisov** • Inquiries: vborisov.alexandrov@gmail.com