Lesson 7.3: Regulating the New – Crypto, AI, and Digital Operational Resilience

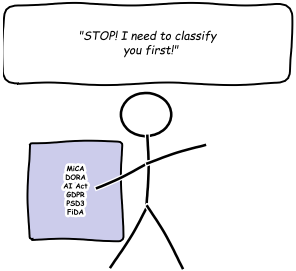
Module 7: The Compliance Problem

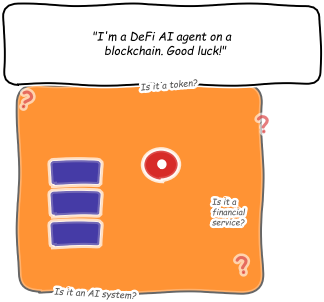
Prof. Dr. Joerg Osterrieder

February 9, 2026

(c) Joerg Osterrieder 2025–2026

Regulating the New: A Candid Look





Regulators: "We have a framework." Innovation: "Hold my private key."

Technology moves at the speed of code; regulation moves at the speed of consensus. The gap between the two creates both risk and opportunity.

Learning Objectives

By the end of this lesson, you will be able to:

1. Describe the EU's Markets in Crypto-Assets (MiCA) regulation and explain how it classifies crypto-assets into EMTs, ARTs, and utility tokens
2. Explain how the EU AI Act assigns risk tiers to AI systems and identify which financial applications fall under "high risk"
3. Outline the five pillars of the Digital Operational Resilience Act (DORA) and explain why ICT risk management now has its own regulation
4. Analyse how GDPR's "right to explanation" constrains algorithmic decision-making in finance
5. Compare crypto and AI regulatory approaches across the EU, US, UK, Singapore, and Switzerland
6. Evaluate the regulatory challenges posed by DeFi, stablecoins, and autonomous AI agents

---

This lesson covers four landmark regulations (MiCA, EU AI Act, DORA, GDPR) and how they interact in the world of digital finance.

Bridge: From Compliance Automation to the Rules Themselves

Where we have been:

- Module 7 Lessons 1–2: How to automate compliance—RegTech, KYC, AML, transaction monitoring
- We built the machinery to enforce rules efficiently
- But *which* rules? The rulebook itself is being rewritten

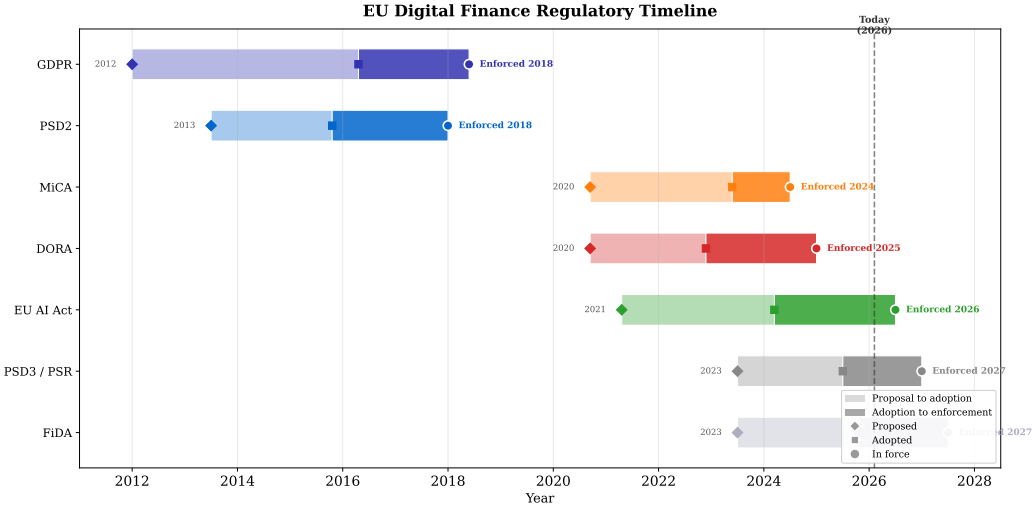
Where we are going:

- This lesson: the **new regulations** that govern crypto-assets, artificial intelligence, and digital operational resilience
- Four pillars: MiCA, EU AI Act, DORA, GDPR
- Cross-jurisdictional comparison

We can automate compliance. But what are the NEW rules we must comply with?

RegTech is the engine; regulation is the fuel. Without understanding MiCA, the AI Act, and DORA, your compliance engine has no map.

The EU's Digital Finance Regulatory Wave



Between 2020 and 2027, the EU enacted or proposed seven major regulations affecting digital finance. Firms must comply with all of them simultaneously.

(c) Joerg Osterrieder 2025–2026

MiCA: Markets in Crypto-Assets Regulation

What is MiCA?

- **Regulation (EU) 2023/1114**: the world's first comprehensive crypto-asset regulatory framework
- Effective June 2024 (stablecoins), December 2024 (full scope)
- Creates a single EU-wide licensing regime—replaces 27 national patchwork approaches

Key principle:

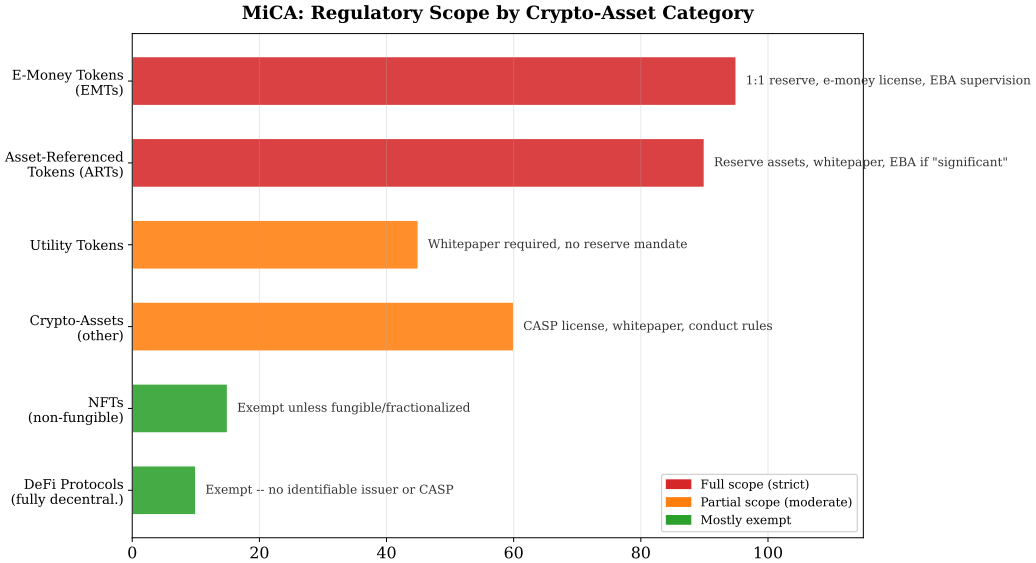
- **Same activity, same risk, same rules**: if a crypto-asset behaves like a financial instrument, it gets regulated like one
- Passporting: one license valid across all 27 EU member states

MiCA classifies crypto-assets into three buckets:

1. **E-Money Tokens (EMTs)**: pegged to a single fiat currency (e.g., a EUR stablecoin). Treated like e-money—1:1 reserve, e-money license required
2. **Asset-Referenced Tokens (ARTs)**: pegged to a basket of assets (e.g., Diem-style). Reserve requirements, EBA supervision if "significant"
3. **Other crypto-assets**: utility tokens and general crypto. Whitepaper required, lighter conduct rules

MiCA is to crypto what MiFID II is to securities: a comprehensive, pan-European regulatory framework that turns the Wild West into a regulated market.

MiCA: Regulatory Scope by Asset Category



MiCA: Crypto-Asset Service Providers (CASPs)

What is a CASP?

- Any entity providing crypto-asset services: custody, exchange, trading, portfolio management, transfer, advice
- Must be **authorized** by a national competent authority (NCA)
- Authorization is "passportable" across the EU

CASP obligations:

- Minimum capital requirements (varies by service: €50K–€150K)
- Governance and organisational requirements
- Complaint handling and conflict of interest rules
- AML/CFT compliance (5AMLD/6AMLD integration)

Key provisions:

- **Whitepaper**: mandatory disclosure document for any public offering of crypto-assets (like a prospectus)
- **Market abuse**: insider dealing and market manipulation rules apply to crypto-assets
- **Liability**: issuers are liable for inaccurate whitepaper information

Who is exempt?

- Already-licensed entities (MiFID firms, credit institutions) can provide CASP services under simplified notification
- ECB, EIB, and public entities
- Fully decentralized protocols with no identifiable service provider (contentious)

MiCA creates a level playing field: crypto exchanges face rules comparable to traditional securities exchanges. The era of unregulated crypto platforms in the EU is over.

MiCA: Stablecoin Regulation – EMTs and ARTs

E-Money Tokens (EMTs):

- Pegged 1:1 to a single fiat currency
- Issuer must be a licensed **credit institution** or **e-money institution**
- **Reserve**: 100% liquid assets, held in custody
- Holders have a **right of redemption** at par at any time
- Example: a EUR stablecoin must be fully backed by EUR-denominated reserves

Asset-Referenced Tokens (ARTs):

- Pegged to a basket of currencies, commodities, or crypto-assets
- Must maintain a robust **reserve of assets**
- If ART becomes "significant" (>€5B market cap or >10M holders), EBA takes over supervision
- Additional requirements: stress testing, wind-down plans, recovery plans

What about Tether (USDT)?

- USDT must comply with EMT rules in the EU
- Several EU exchanges delisted non-compliant stablecoins in late 2024
- Compliance deadline forced market restructuring

The collapse of TerraUSD ($40B lost in May 2022) demonstrated why stablecoin reserves matter. MiCA's reserve rules are a direct response to that failure.

The EU AI Act: World's First Comprehensive AI Regulation

What is the EU AI Act?

- **Regulation (EU) 2024/1689**: entered into force August 2024
- Phased enforcement: bans in Feb 2025, high-risk rules by Aug 2026
- Applies to any AI system placed on the EU market or whose output is used in the EU
- Extraterritorial scope (like GDPR)

Key principle: risk-based approach

- Regulation proportional to the risk an AI system poses
- Four tiers: unacceptable, high, limited, minimal
- Most AI systems fall into "minimal risk" with no obligations

Why it matters for finance:

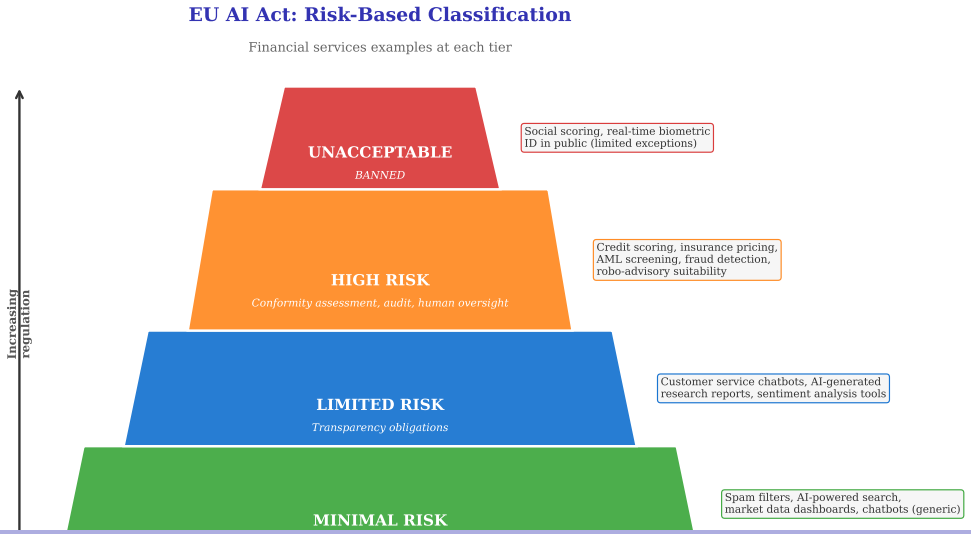
- Credit scoring → **high risk**
- Insurance pricing → **high risk**
- AML/fraud detection → **high risk**
- Robo-advisory suitability → **high risk**
- Customer service chatbot → **limited risk**
- Internal analytics → **minimal risk**

Penalties:

- Up to €35M or 7% of global turnover (banned systems)
- Up to €15M or 3% of turnover (high-risk non-compliance)

The EU AI Act regulates the use of AI, not the technology itself. A neural network used for spam filtering is unregulated; the same architecture used for credit scoring is high-risk.

EU AI Act: Risk Classification Pyramid



High-Risk AI in Financial Services

What makes a financial AI "high-risk"?

- Listed in **Annex III, Section 5(b)**: "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score"
- Also: systems used to "evaluate and classify emergency calls" and "assess eligibility for public benefits" (by analogy: insurance, lending, welfare)

High-risk obligations:

1. **Risk management system** (ongoing, documented)
2. **Data governance**: training data must be representative, free from bias
3. **Technical documentation**: full system description, design choices, performance metrics

High-risk obligations (continued):

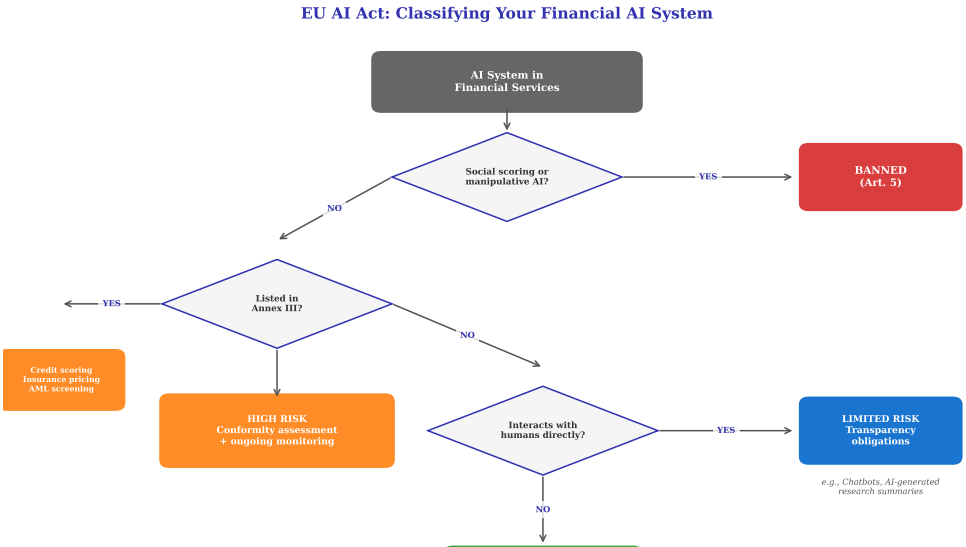
4. **Record-keeping**: automatic logging of system operations
5. **Transparency**: users informed they are interacting with AI
6. **Human oversight**: "meaningful" human-in-the-loop or human-on-the-loop capability
7. **Accuracy, robustness, cybersecurity**: documented performance benchmarks

Conformity assessment:

- Self-assessment for most high-risk systems (including financial AI)
- Notified body assessment for biometric systems
- Registration in EU database before market placement

A bank's credit scoring model must now have documented training data, bias testing, performance benchmarks, and a human override mechanism—before it can be deployed.

Decision Tree: Classifying Your Financial AI System



The AI Act Meets GDPR: Double Regulation

GDPR already regulates AI in finance:

- **Article 22**: right not to be subject to decisions based solely on automated processing that produce legal or significant effects
- **Recital 71**: right to obtain "meaningful information about the logic involved" (the "right to explanation")
- **Article 35**: Data Protection Impact Assessment (DPIA) required for high-risk processing

How AI Act adds to GDPR:

- GDPR focuses on **data protection** (personal data rights)
- AI Act focuses on **system safety** (risk to fundamental rights)
- Both apply simultaneously—firms must comply with both
- AI Act adds: technical documentation, conformity assessment, post-market monitoring
- GDPR adds: consent, purpose limitation, right to erasure

Practical conflict:

- AI Act requires *representative training data*
- GDPR requires *data minimization*
- Firms must balance both

A credit scoring AI must satisfy both: GDPR's right to explanation AND the AI Act's conformity assessment. Compliance teams need to understand both frameworks together.

DORA: Digital Operational Resilience Act

What is DORA?

- **Regulation (EU) 2022/2554**: entered into force January 2025
- Applies to all EU financial entities: banks, insurers, investment firms, payment institutions, crypto-asset service providers
- Also applies to **critical ICT third-party providers** (cloud, data, software vendors)

Why DORA?

- Finance depends on ICT infrastructure (cloud, APIs, software)
- A cloud outage at a single provider can disrupt millions of customers
- Before DORA: ICT risk was covered by general risk rules—not specific enough

DORA's scope:

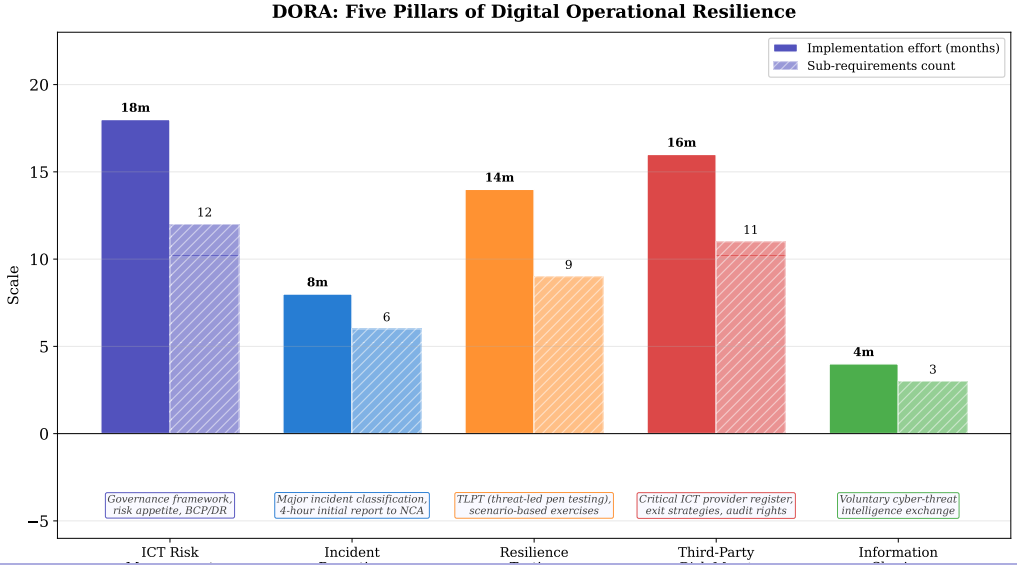
- >22,000 financial entities in the EU
- >15,000 ICT service providers
- First regulation to give supervisors **direct oversight** of critical ICT providers (AWS, Azure, Google Cloud)

Key distinction:

- DORA is a **regulation** (directly applicable in all member states), not a directive (requires transposition)
- Harmonized across the EU—no national gold-plating
- Proportionality: smaller firms face lighter requirements

DORA recognizes that in 2025, operational resilience IS digital resilience. A bank's ability to serve customers depends on its ICT infrastructure more than its physical branches.

DORA: The Five Pillars of Digital Operational Resilience



DORA: Pillar-by-Pillar Requirements

Pillar	Key Requirements	Practical Impact
ICT Risk Mgmt	Governance framework, risk appetite statement, BCP/DR plans, annual review	Board-level accountability for ICT risk; CTO/CISO must report to board
Incident Reporting	Classify incidents (major/significant), initial report within 4 hours to NCA, root-cause analysis	Standardized incident taxonomy; faster disclosure than before
Resilience Testing	Regular vulnerability scans, advanced TLPT (threat-led penetration testing) every 3 years	Large firms must run Red Team exercises; test results shared with supervisor
Third-Party Risk	Register of all ICT providers, due diligence, contractual exit strategies, audit rights	Cannot outsource accountability; must plan for provider failure
Info Sharing	Voluntary cyber-threat intelligence exchange between financial entities	Encourages collective defence; safe harbour for shared threat data

DORA's third-party risk pillar is transformative: for the first time, regulators can directly supervise cloud providers like AWS and Google Cloud when they serve financial firms.

DORA: Critical ICT Third-Party Providers

What is a "critical" provider?

- Designated by European Supervisory Authorities (EBA, ESMA, EIOPA)
- Criteria: systemic importance, degree of substitutability, concentration risk
- Expected: AWS, Microsoft Azure, Google Cloud, Snowflake, major SaaS platforms

Oversight powers:

- Lead Overseer appointed (one ESA per provider)
- On-site inspections of the ICT provider
- Recommendations (non-binding but "comply or explain")
- If provider refuses: financial entities must consider exit

Concentration risk:

- If 80% of EU banks use AWS, an AWS outage is a systemic event
- DORA requires firms to assess and document concentration risk
- Multi-cloud strategies become a compliance consideration, not just an architecture choice

Exit strategies:

- Every outsourcing contract must include exit and transition plans
- Data portability and repatriation within defined timeframes
- "No lock-in" becomes a regulatory mandate

DORA transforms cloud risk from a procurement issue into a regulatory obligation. Firms must prove they can survive the failure of any single ICT provider.

GDPR: The Right to Explanation in Financial AI

Article 22: Automated Decision-Making

- Data subjects have the right "not to be subject to a decision based solely on automated processing ... which produces legal effects"
- Financial decisions (loan approval, insurance pricing, fraud flagging) clearly qualify
- Exceptions: explicit consent, contract necessity, or law

Recital 71: "Right to Explanation"

- Data subjects may "obtain an explanation of the decision reached after such assessment"
- Legal scholars debate: is this a right to the *logic* or the *specific factors* in your case?
- Practical consequence: black-box models are risky under GDPR

Practical implications for financial firms:

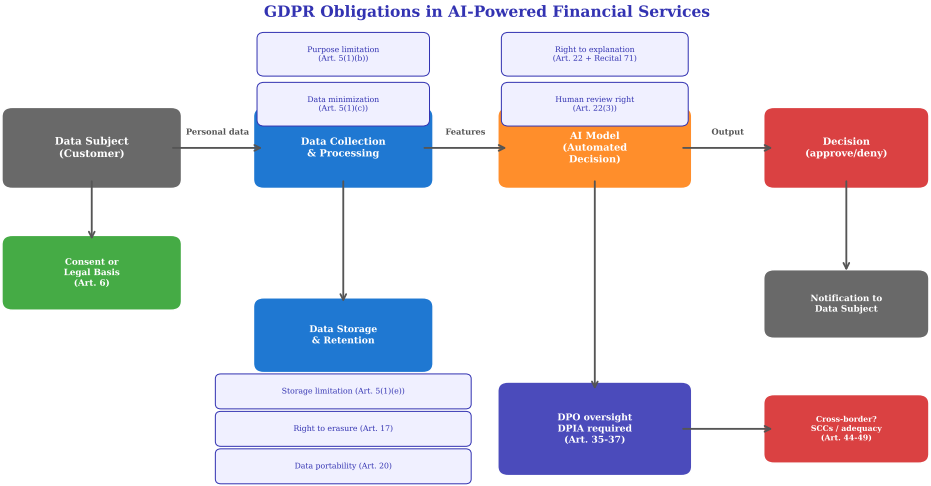
- Must provide "meaningful information about the logic involved, as well as the significance and envisaged consequences" (Art. 13(2)(f))
- Human review must be available on request
- Firms must disclose that automated processing is used *before* it happens

Model choice consequences:

- **Logistic regression**: easily explainable ✓
- **Decision tree (shallow)**: transparent ✓
- **XGBoost + SHAP**: defensible with explainability tools
- **Deep neural network**: requires significant post-hoc explanation effort

GDPR's right to explanation does not ban complex models—but it requires firms to invest in explainability. SHAP, LIME, and counterfactual explanations are compliance tools, not just research.

GDPR: Data Flow Through Financial AI Systems



Stablecoin Regulation: Why It Matters

The TerraUSD collapse (May 2022):

- TerraUSD (UST) was an **algorithmic stablecoin**: no fiat reserves, maintained peg through a mint/burn mechanism with LUNA
- Death spiral: UST lost peg → LUNA hyperinflated → both crashed to zero
- **$40 billion** in value destroyed in 72 hours
- Contagion: Three Arrows Capital, Celsius, Voyager Digital all collapsed

Regulatory response:

- MiCA explicitly bans algorithmic stablecoins that rely solely on protocol mechanisms
- Requires **full asset backing** for EMTs and ARTs
- Issuers must hold reserves in segregated, highly liquid assets
- Mandatory redemption at par value at all times

Global stablecoin regulation:

- US: proposed legislation (unclear timeline)
- UK: FCA regulating as "fiat-backed stablecoins" from 2025
- Singapore: MAS framework for single-currency stablecoins
- FSB: global recommendations (2023)

TerraUSD proved that "stable" is a promise, not a property. Without reserves, stability depends on confidence—and confidence can evaporate in hours.

EU DLT Pilot Regime: Experimenting with Regulation

What is the DLT Pilot Regime?

- **Regulation (EU) 2022/858**: effective March 2023
- A regulatory "sandbox" allowing firms to trade and settle **DLT-based financial instruments** under relaxed MiFID/CSDR rules
- Duration: 6 years (can be extended)

What it allows:

- Tokenized equities and bonds traded on DLT
- Combined trading and settlement (T+0 potential)
- Exemptions from certain CSD requirements
- Market cap limit: €500M per issuer, €6B total on any DLT platform

Why it matters:

- Tests whether DLT can replace traditional post-trade infrastructure
- Real regulatory exemptions for real market participants
- Lessons feed back into future regulation ("evidence-based policymaking")

Limitations:

- Only for "DLT financial instruments" (not crypto-assets generally)
- Caps on volume and market cap
- Participants must be licensed under MiFID
- Early days: limited adoption as of 2025

The DLT Pilot Regime is the EU's way of saying: "We see the potential of tokenized securities. Let us test it under controlled conditions before rewriting the rulebook."

DeFi: The Regulatory Blind Spot

Why DeFi is hard to regulate:

- **No identifiable entity**: who is the "service provider" of Uniswap?
- Smart contracts execute autonomously—no human in the loop
- Pseudonymous participants, borderless operations
- MiCA explicitly excludes "fully decentralized" protocols—but admits this is a temporary gap

DeFi regulation attempts:

- US SEC: treats many DeFi tokens as securities (enforcement-led approach)
- EU: MiCA review by 2027 must address DeFi
- FATF: "virtual asset service provider" (VASP) definition may expand to include DeFi front-ends

Emerging regulatory hooks:

- **Front-end regulation**: regulate the website/app, not the protocol
- **Governance token holders**: treat them as responsible parties
- **KYC gateways**: require identity verification before protocol interaction
- **Compliance by design**: embed regulatory logic in smart contracts

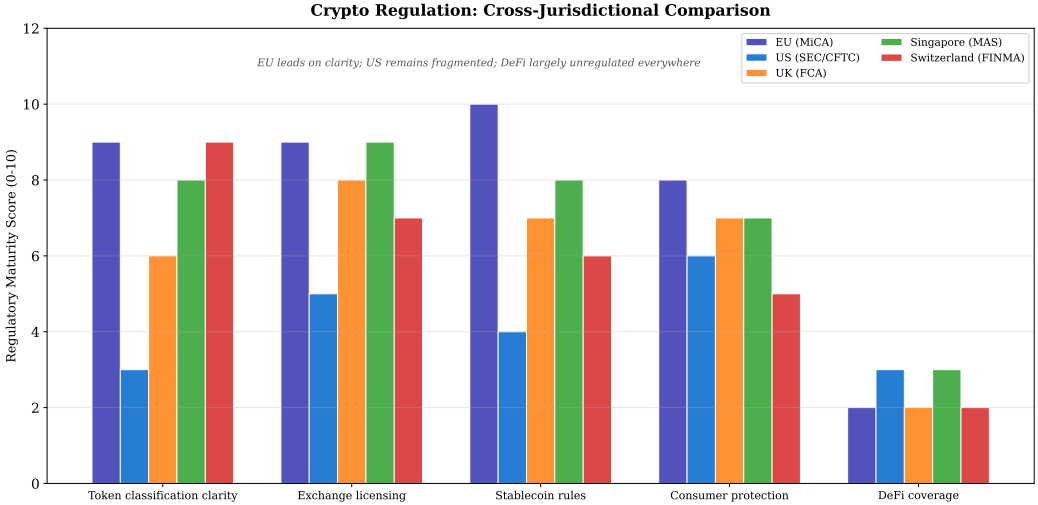
The paradox:

- Regulating DeFi defeats its purpose (decentralization)
- Not regulating creates a $100B+ unregulated financial system
- Likely outcome: "CeDeFi"—centralized front-ends, decentralized back-ends

DeFi is the hardest regulatory challenge in digital finance: the rules assume an identifiable entity to regulate. DeFi removes the entity. Regulators must find new anchoring points.

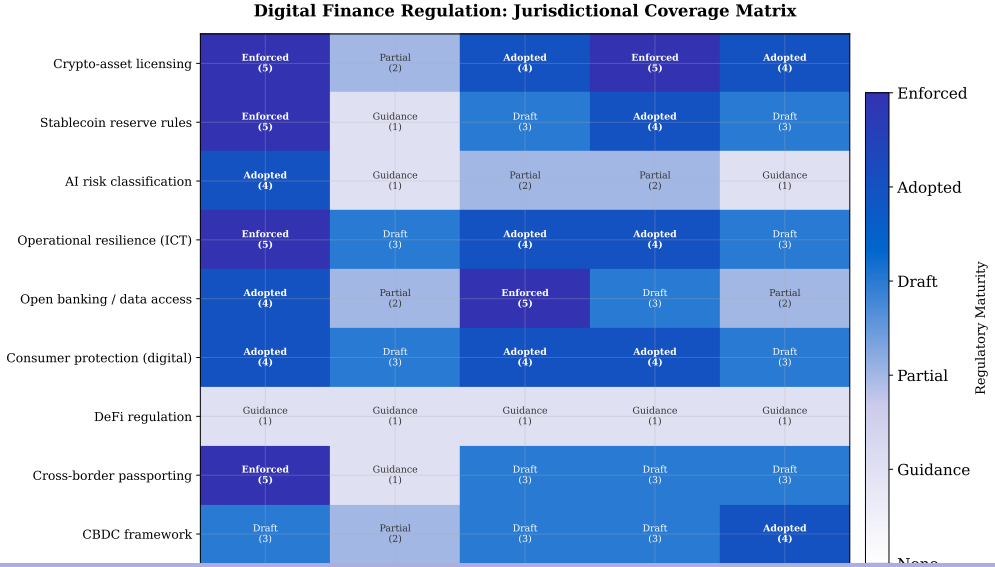
(c) Joerg Osterrieder 2025–2026

Crypto Regulation: A Global Comparison



The EU leads on regulatory clarity with MiCA. The US remains fragmented between SEC and CFTC. DeFi is a blind spot everywhere.

Digital Finance Regulation: Jurisdictional Coverage



Regulatory Philosophy: EU vs. US

Dimension	EU (principles-based)	US (enforcement-led)
Crypto classification	MiCA: clear taxonomy (EMT, ART, utility)	SEC vs. CFTC jurisdictional battle; Howey Test case-by-case
AI regulation	EU AI Act: horizontal, risk-based framework	No federal AI law; sector-specific guidance; state-level laws
Operational resilience	DORA: unified, cross-sector	OCC/FFIEC guidance; no single framework
Stablecoins	MiCA: reserve rules, licensing	Proposed legislation stalled; enforcement actions ad hoc
Passporting	Single license valid across 27 states	State-by-state money transmitter licenses
Enforcement style	Ex-ante rules (regulate first)	Ex-post enforcement (sue first, regulate later)

The EU regulates before problems arise (precautionary principle). The US lets markets develop and sues bad actors after the fact. Both approaches have trade-offs.

Regulatory Intersections: When Four Regulations Collide

Case study: AI-powered crypto lending platform
A platform uses ML to score borrowers and automatically approves crypto-backed loans. Which regulations apply?

1. **MiCA**: platform is a CASP offering crypto lending; needs authorization and whitepaper
2. **EU AI Act**: credit scoring model is high-risk; conformity assessment, human oversight, documentation
3. **GDPR**: personal data processed; right to explanation, DPIA, data minimization
4. **DORA**: operational resilience of the platform's ICT infrastructure; incident reporting, third-party risk

Practical compliance stack:

- **Legal**: CASP authorization + AI Act registration + GDPR records of processing
- **Technical**: model documentation + DPIA + ICT risk framework + incident reporting
- **Organizational**: DPO + AI compliance officer + CISO + board reporting
- **Ongoing**: post-market monitoring (AI Act) + periodic resilience testing (DORA) + data subject requests (GDPR)

Cost estimate:

- Large bank: €5–15M for combined compliance
- Mid-size fintech: €500K–2M
- Startup: potentially prohibitive without RegTech automation

No regulation exists in isolation. A single product can trigger four or more regulatory frameworks. This is why cross-functional compliance teams and RegTech automation are essential.

Emerging Regulatory Challenges

AI agents and autonomous systems:

- AI agents that trade, lend, or manage portfolios autonomously
- Who is liable when an AI agent makes a bad trade?
- EU AI Act covers "general-purpose AI" models but not autonomous agents specifically
- OpenAI, Anthropic, and others are deploying agents in finance

Tokenization of real-world assets:

- Tokenized bonds, equities, real estate
- MiFID or MiCA? Depends on whether the token qualifies as a "financial instrument"
- DLT Pilot Regime is a partial answer

CBDCs (Central Bank Digital Currencies):

- Digital euro proposal (2023): not crypto, not a stablecoin, but a new category
- Requires new privacy rules, offline capability, holding limits
- Interaction with MiCA: CBDCs are explicitly excluded from MiCA scope

Regulatory sandboxes:

- EU AI Act Article 57: member states must establish AI regulatory sandboxes
- Allow testing under supervisory oversight
- Reduced compliance burden during sandbox period
- Similar to FCA sandbox (UK), MAS sandbox (Singapore)

Regulation always lags innovation. The key question is whether today's frameworks are flexible enough to accommodate tomorrow's technology—or whether they will need to be rewritten again.

Key Takeaways

1. **MiCA** creates the world's first comprehensive crypto-asset framework: EMTs, ARTs, utility tokens, CASPs, whitepapers, and passporting across 27 EU states
2. **The EU AI Act** introduces risk-based AI regulation: credit scoring, AML, and insurance pricing are all "high-risk" requiring conformity assessment and human oversight
3. **DORA** makes digital operational resilience a legal obligation: five pillars covering ICT risk, incident reporting, resilience testing, third-party risk, and information sharing
4. **GDPR's Article 22** gives individuals the right to explanation and human review of automated financial decisions—constraining black-box models
5. **These regulations interact**: a single financial product can trigger MiCA + AI Act + GDPR + DORA simultaneously
6. **The EU leads on clarity**; the US remains fragmented; DeFi is a regulatory blind spot everywhere
7. **Regulatory sandboxes** allow controlled innovation: DLT Pilot Regime, AI sandboxes, and national fintech sandboxes
8. **Compliance cost is significant** but RegTech automation (Lesson 7.1–7.2) makes it manageable

---

The regulatory landscape for digital finance is the most complex it has ever been. Understanding it is not optional—it is a competitive advantage.

Summary: Lesson 7.3

Concepts covered:

- MiCA: crypto-asset classification, CASPs, stablecoin rules, whitepapers, passporting
- EU AI Act: risk pyramid, high-risk financial AI, conformity assessment, penalties
- DORA: five pillars, critical ICT provider oversight, concentration risk, exit strategies
- GDPR: Article 22, right to explanation, DPIA, model choice implications
- Stablecoin regulation post-TerraUSD
- DLT Pilot Regime and DeFi regulatory gaps
- Cross-jurisdictional comparison (EU, US, UK, SG, CH)
- Regulatory interactions and emerging challenges

What comes next:

- Lesson 7.4: Building a compliance-first culture—governance frameworks, three lines of defence, regulatory reporting

Practical advice:

- Map every product to its regulatory triggers (MiCA, AI Act, DORA, GDPR)
- Build compliance into the design, not as an afterthought
- Invest in explainability—it satisfies both GDPR and the AI Act
- Plan for multi-regulation: one product, four frameworks
- Use regulatory sandboxes to test before full compliance investment

Regulating the new is hard. But understanding the rules gives you a head start—over competitors who treat compliance as a cost rather than a capability.