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

Prof. Dr. Joerg Osterrieder

Exercise 1: MiCA Classification Challenge

Classify each of the following crypto-assets under MiCA and identify the regulatory requirements:

1. A token pegged 1:1 to the euro, issued by a licensed e-money institution, redeemable at par
2. A token backed by a basket of 50% USD, 30% EUR, and 20% gold
3. A token that grants access to a decentralized cloud storage network
4. A digital collectible representing a unique piece of artwork (one-of-one)
5. A governance token for a fully decentralized lending protocol where no single entity controls the smart contracts
6. A token pegged to the Swiss franc issued by a Singapore-based company with EU customers

For each, specify:

- MiCA category (EMT, ART, utility, NFT, or exempt)
- Required license type (if any)
- Whether a whitepaper is mandatory
- Whether EBA or NCA supervision applies

Exercise 2: EU AI Act Risk Assessment for a Bank

A mid-size European bank uses AI in the following ways. For each application, determine the EU AI Act risk tier and the obligations that apply:

1. A model that scores mortgage applicants and recommends approval or denial
2. A chatbot on the bank's website that answers frequently asked questions about account fees
3. An internal tool that summarizes earnings call transcripts for analysts
4. A system that monitors transactions and flags suspicious activity for AML investigators
5. An AI-powered camera system in the lobby that identifies customers by face for "VIP" routing
6. A recommendation engine that suggests investment products to retail clients based on their risk profile

For each high-risk system, outline:

- What technical documentation is required
- What human oversight mechanism would satisfy the regulation
- How the bank would conduct the conformity assessment

Exercise 3: DORA Compliance Gap Analysis

A fintech payment institution currently has the following ICT setup:

- All infrastructure on AWS (single cloud provider)
- Incident response plan documented but untested
- No formal register of ICT third-party providers
- Annual penetration test by external firm
- No formal ICT risk appetite statement approved by the board

Tasks:

1. Map each of the five DORA pillars to the firm's current state. For each pillar, identify: (a) what is already in place, (b) what is missing, and (c) what must change
2. The firm uses AWS exclusively. Under DORA's third-party risk rules, what specific actions must the firm take regarding concentration risk?
3. Design an incident classification scheme that distinguishes "major" from "significant" ICT incidents, with examples of each
4. The board asks: "How much will DORA compliance cost us?" Provide a rough estimate broken down by pillar, assuming 50 employees and €80/hour average cost

Exercise 4: GDPR vs. AI Act – The Explainability Challenge

A bank's credit scoring model uses XGBoost with 150 features to predict default probability. A customer named Maria is denied a loan and demands an explanation.

Tasks:

1. Under GDPR Article 22, what information must the bank provide to Maria? Be specific about what "meaningful information about the logic involved" means in practice.
2. Under the EU AI Act, what additional documentation must exist for this high-risk system? List at least five specific requirements.
3. Maria's denial was primarily driven by: (a) low income, (b) short credit history, and (c) high debt-to-income ratio. Draft a compliant explanation letter that satisfies both GDPR and the AI Act.
4. The bank considers switching to a deep neural network for better accuracy. What additional explainability challenges would this create under GDPR? What tools (SHAP, LIME, counterfactuals) would you recommend and why?
5. The GDPR requires data minimization, but the AI Act requires representative training data. Maria's application included her nationality and gender. Should these features be included in the model? Argue both sides.

Exercise 5: Stablecoin Compliance Simulation

A Swiss fintech company wants to issue a EUR-pegged stablecoin ("EuroStable") and offer it to EU customers via exchanges.

Tasks:

1. Under MiCA, classify EuroStable. What license does the issuer need? Can a Swiss company obtain this license?
2. Design the reserve structure: What assets can back EuroStable? What percentage must be in bank deposits vs. government bonds? Where must reserves be held?
3. EuroStable reaches €6 billion market cap and 12 million holders. What changes in its regulatory status? Which supervisor takes over?
4. A competing stablecoin ("AlgoEUR") maintains its peg through an algorithmic mint/burn mechanism with no asset reserves. Explain why MiCA prohibits this design. Reference the TerraUSD collapse.
5. Calculate the compliance cost: licensing (€200K), legal counsel (€150K/year), custody fees (0.1% of reserves), audit (2x/year at €50K each), reporting systems (€100K). What is the minimum reserve size at which EuroStable breaks even if it earns 3% yield on reserves?

Exercise 6: Cross-Jurisdictional Regulatory Arbitrage

A crypto trading platform operates globally and must decide where to establish its legal headquarters.

Factor	EU (MiCA)	US (SEC/CFTC)	Singapore (MAS)
License cost	€150K + ongoing	$500K+ legal fees	SGD 250K
Time to license	6–12 months	18–36 months	6–9 months
Market access	450M people, 27 countries	330M people, 1 country	6M local, APAC gateway
Stablecoin rules	Clear (MiCA)	Unclear (proposed)	Clear (MAS framework)
DeFi stance	Exempt (for now)	Hostile (enforcement)	Cautious (case-by-case)

Tasks:

1. For each jurisdiction, calculate a "regulatory cost-benefit score" using the factors above. Weight market access at 40%, regulatory clarity at 30%, cost at 20%, speed at 10%.
2. The platform plans to offer: spot trading, staking, and a DeFi aggregator. Which jurisdiction is best for each product? Can the platform use different jurisdictions for different products?
3. What is "regulatory arbitrage" and why do regulators view it negatively? How does MiCA's passporting reduce the incentive for intra-EU regulatory arbitrage?

Exercise 7: Multi-Regulation Compliance Mapping

A European fintech launches an AI-powered crypto lending platform. Map the full regulatory compliance requirements.

Product description:

- Accepts crypto collateral (BTC, ETH) and issues EUR stablecoin loans
- Uses an ML model to assess borrower creditworthiness
- Operates on cloud infrastructure (AWS + Google Cloud)
- Serves retail customers across 10 EU member states

Tasks:

1. Create a compliance matrix: rows = regulations (MiCA, AI Act, DORA, GDPR, 5AMLD), columns = requirements, cells = specific obligations
2. Identify three areas where regulations *conflict* or create tension (e.g., GDPR data minimization vs. AI Act representative data). Propose solutions.
3. Design the organizational structure: which compliance roles are needed? (DPO, CISO, AI compliance officer, MLRO, etc.) Can roles be combined?
4. Estimate total annual compliance cost (staff, technology, legal, audit). Compare this to a traditional bank offering the same product—is the fintech at a disadvantage?

Exercise 8: The Future of DeFi Regulation

The European Commission has asked you to draft a policy brief on DeFi regulation for the MiCA review (due 2027).

Tasks:

1. Describe the three main regulatory approaches to DeFi:
   - Front-end regulation (regulate the website/app)
   - Governance token holder liability (treat token holders as responsible)
   - Embedded compliance (regulatory logic in smart contracts)

   For each, list two advantages and two disadvantages.
2. A lending protocol has $5B TVL, 100K users, and no identifiable team. A user loses funds due to a smart contract bug. Under current EU law, who (if anyone) is liable? What would you change?
3. Design a "DeFi Pilot Regime" (analogous to the DLT Pilot Regime): what exemptions would you grant? What safeguards would you require? What metrics would determine success?
4. The industry argues that regulating DeFi will push innovation outside the EU. Evaluate this claim. Does the precedent of GDPR (which initially faced similar criticism) support or undermine this argument?

Answer Key (1/3)

Exercise 1: 1) EMT: e-money license, whitepaper, 1:1 reserve, NCA supervision. 2) ART: credit institution license, whitepaper, basket reserve, NCA (EBA if significant). 3) Utility token: whitepaper required, lighter conduct rules, NCA. 4) NFT: exempt from MiCA (unique, non-fungible, not fractionalized). 5) Exempt: fully decentralized, no identifiable issuer or CASP. 6) EMT: the Swiss issuer must obtain an EU e-money license (or partner with an EU-licensed entity) to serve EU customers.

Exercise 2: 1) Mortgage scoring: HIGH RISK (Annex III, creditworthiness). Requires: risk management system, data governance, technical documentation, logging, human oversight (loan officer can override), conformity self-assessment. 2) FAQ chatbot: LIMITED RISK. Must disclose AI interaction to users. 3) Internal summarization: MINIMAL RISK. No obligations. 4) AML monitoring: HIGH RISK. Same as mortgage scoring; human investigator reviews flagged transactions. 5) Facial recognition for VIP routing: potentially UNACCEPTABLE if real-time biometric identification in publicly accessible space. Must verify exemption applicability. 6) Investment recommendation: HIGH RISK (if it produces legally significant effects on investment decisions). Conformity assessment, human-on-the-loop.

Answer Key (2/3)

Exercise 3: 1) Pillar mapping: ICT Risk Mgmt – missing risk appetite statement and board approval. Incident Reporting – plan exists but untested, no classification scheme. Resilience Testing – annual pen test exists but TLPT not done. Third-Party Risk – no register, no exit strategy for AWS. Info Sharing – not in place. 2) Concentration risk actions: create ICT provider register, document AWS dependency, assess substitutability, negotiate contractual exit clause with data portability, consider secondary cloud provider for critical workloads. 3) Major: total platform outage $>$2 hours, data breach affecting $>$1,000 customers. Significant: partial service degradation, security incident contained without data loss. 4) Cost estimate: ICT Risk Mgmt $\approx$400 hours (€32K), Incident Reporting $\approx$200h (€16K), Testing $\approx$300h (€24K) + external TLPT (€50K), Third-Party Risk $\approx$250h (€20K), Info Sharing $\approx$50h (€4K). Total $\approx$€146K first year.

Exercise 4: 1) GDPR requires: the fact that automated processing was used, the logic involved (top factors influencing the decision), significance and consequences, right to contest and obtain human review. 2) AI Act requires: system description, design choices, training data description and bias analysis, performance metrics (accuracy, FPR, FNR), risk management documentation, human oversight mechanism. 3) Explanation letter should state: "Your application was assessed using an automated credit scoring system. The main factors were: (1) income below threshold, (2) credit history $<$2 years, (3) debt-to-income ratio above 45%. You may request a human review." 4) DNNs are harder to explain. SHAP provides feature attribution; LIME provides local approximations; counterfactual explanations ("If your income were €5K higher, the decision would change") are most intuitive for customers.

Answer Key (3/3)

Exercise 5: 1) EMT classification. Swiss company needs an EU e-money license (must establish EU subsidiary or partner). 2) MiCA Art. 36: $\geq$30% in bank deposits, remainder in high-quality government bonds. Reserves held by EU-based custodian, segregated. 3) At €6B+ market cap and >10M holders, EuroStable is "significant": EBA takes over supervision, additional stress testing, recovery plan, wind-down plan. 4) MiCA Art. 44: algorithmic stablecoins without asset reserves are prohibited because the peg depends on market confidence. TerraUSD showed this confidence can collapse in hours. 5) Annual costs: €200K (license amortized) + €150K (legal) + 0.1% reserves (custody) + €100K (audit) + €100K (systems) = €550K + 0.1% reserves. At 3% yield, breakeven: $0.03R - 0.001R - 550{,}000 = 0$, so $R = e550{,}000/0.029 \approx$ €19M.

Exercise 6: 1) Scoring example: EU = 0.4(10)+0.3(9)+0.2(6)+0.1(6) = 8.5. US = 0.4(8)+0.3(3)+0.2(4)+0.1(3) = 5.2. Singapore = 0.4(4)+0.3(8)+0.2(7)+0.1(8) = 5.8. 2) Spot trading: EU (passporting, clear rules). Staking: Singapore (pragmatic). DeFi aggregator: Singapore (cautious but not hostile). Multi-entity structure possible but adds complexity. 3) Regulatory arbitrage: choosing jurisdictions with lightest rules. MiCA passporting eliminates intra-EU arbitrage incentive since one license covers all member states.

Exercise 7: Compliance matrix should show: MiCA (CASP license, stablecoin issuance rules), AI Act (credit model is high-risk), DORA (ICT resilience, multi-cloud), GDPR (personal data, DPIA, Art. 22), 5AMLD (KYC/AML). Conflicts: data minimization vs. representative data, solved with synthetic data; retention limits vs. audit trails, solved with anonymization schedules.

Exercise 8: Front-end regulation: pro (enforceable, clear target), con (easily circumvented, kills UX). Governance holders: pro (creates accountability), con (may discourage governance participation, hard to identify). Embedded compliance: pro (scalable, automated), con (technically difficult, smart contract bugs). GDPR precedent: initial "innovation flight" fears were overstated; GDPR became a global standard.