Module 7 Summary: The Compliance Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Module 7: Prerequisites

Theme: Compliance (AML/KYC, RegTech, regulating new, model risk) **From prior modules:**

- **M3L3:** smart-contract audit context
- **M5L1:** ML model outputs as supervisory artefacts
- **M5L4:** MLOps as the operating context for model risk

External knowledge assumed:

- Policy-reasoning literacy: the difference between a rule and a principle
- Light legal primer: regulation vs. supervision vs. enforcement
- Comfort reading regulatory text excerpts (no formal law training)

Will be introduced this module: We introduce AML/KYC fundamentals, RegTech tooling, the EU AI Act and MiCA framework, and SR 11-7 style model-risk governance for institutional ML.

Prerequisites are advisory; lessons remain self-contained where feasible. Forward references inside lessons flag any concept used before its canonical introduction.

Key Concepts by Lesson

L1: AML, KYC & Financial Crime

- AML framework: CDD, EDD, SAR filing
- FATF 40 Recommendations: global standard
- Three stages of laundering: placement, layering, integration
- KYC as barrier to financial inclusion

L2: RegTech

- RegTech = technology solutions for regulatory compliance
- Functional categories: identity, monitoring, reporting, risk
- Automates costly manual processes at scale
- FCA Innovation Hub pioneered RegTech as a sector

L3: Regulating the New

- MiCA: EMTs, ARTs, utility tokens classification
- EU AI Act: high-risk classification for credit scoring
- DORA: operational resilience for financial entities
- GDPR "right to explanation" constrains algorithmic decisions

L4: Model Risk Governance

- SR 11-7: foundational US model risk guidance (2011)
- Three lines of defense: business, risk, audit
- Model risk = incorrect outputs + misuse of correct outputs
- PRA SS1/23: UK equivalent (2024)

Module 7 answers: How do we prevent financial crime and govern algorithmic decision-making without stifling innovation?

Key Formulas and Definitions

AML Framework

CDD (Customer Due Diligence): Standard identity verification at onboarding.
EDD (Enhanced Due Diligence): Deeper scrutiny for high-risk customers (PEPs, high-risk jurisdictions).
SAR (Suspicious Activity Report): Filed with the Financial Intelligence Unit when transactions trigger red flags.

MiCA Token Classification

EMT (E-Money Token): References a single fiat currency (e.g., USDC, EUROC). Regulated like e-money.
ART (Asset-Referenced Token): References multiple assets or currencies. Stricter reserve requirements.
Utility Token: Provides access to a service on a DLT platform. Lightest regulation.

SR 11-7 Model Risk Definition

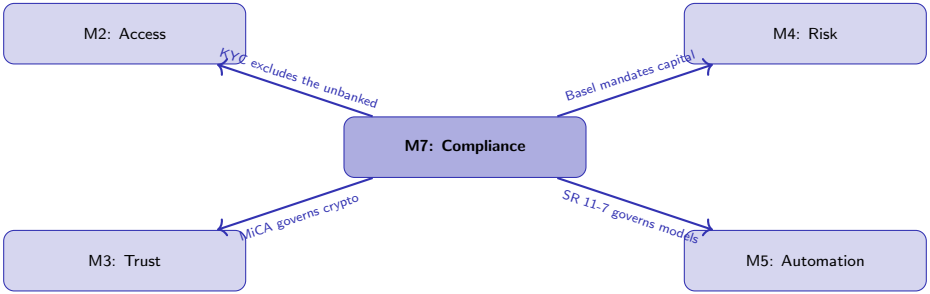
"The potential for adverse consequences from decisions based on incorrect or misused model outputs and reports." Risk arises from: (1) model development errors, (2) incorrect implementation, (3) inappropriate use.

Three Lines of Defense

1st Line: Business units (model owners). **2nd Line:** Risk management (independent validation). **3rd Line:** Internal audit (assurance).

Regulation reacts to crises: Basel after bank failures, AML after scandals, MiCA after crypto collapses, SR 11-7 after model failures.

Connections to Other Modules



- **Compliance → Access (M2):** KYC requirements designed for crime prevention exclude 1.4 billion people without formal identity documents
- **Compliance → Trust (M3):** MiCA creates the first comprehensive crypto-asset regulatory framework, classifying tokens and requiring reserves
- **Compliance → Risk (M4):** Basel III/IV sets minimum capital requirements; each revision responded to a financial crisis
- **Compliance → Automation (M5):** SR 11-7 and the EU AI Act impose governance requirements on ML models used in financial decisions

Compliance is the tension between safety and access: every rule that prevents crime also raises the barrier to entry.

Module 7: Integrative Questions

Two questions that need more than one lesson to answer:

1. M7L1 (AML/KYC) and M7L4 (model-risk governance) appear unrelated; identify two finance workflows where M7L4 governs an M5 model that performs an M7L1 control.
2. Combine M7L2 (RegTech) + M7L3 (regulating the new) to explain why DORA (M7L3) makes RegTech vendor concentration an operational risk in itself.

Use these as study prompts before the module exam; each integrates concepts that span lessons.

Module 7: Worked Multi-Lesson Example

Worked example: a bank deploys a transaction-monitoring model. Trace M7L1 (KYC + watchlist screening), M7L2 (RegTech pipeline + sanctions API), M7L3 (DORA register of ICT third-party providers), M7L4 (SR 11-7 style model lifecycle for the monitoring model). **Pedagogical pattern:** the example is intentionally end-to-end. Solve it lesson-by-lesson, then step back and identify the lesson whose assumption was the binding constraint.

The exam-style version of this example appears in extttv4/exam_prep/exam_bank.tex for module 7.

Module 7: Forward-Pointing Dependency Map

Concepts from Module 7 that later modules will use:

- **M8L1:** Digital identity (M8L1) is the upstream signal for M7L1 KYC at the wallet level
- **M8L3:** ESG disclosure regimes (M8L3) extend M7L3 from prudential to sustainability supervision
- **M5L4:** MLOps (M5L4) is the daily practice that produces the evidence M7L4 governance requires

Forward-pointing dependencies; concepts not in this map are local to Module 7.