AI Compliance for Digital Assets & Crypto

Taught by someone who has built digital-asset systems — exchange, custody and DeFi — and brings AI into crypto compliance work.

WHO IT'S FOR	FORMAT	LENGTH
Founders, MLROs and Heads of Risk at exchanges, custody providers and digital-asset firms.	In-house workshop	Half-day or full-day

What your team walks away with

Bring AI into your compliance and financial-crime work without creating new regulatory exposure — and explain it to your regulator.

What you'll learn

- ✓ Judge where AI genuinely helps your crypto compliance work and where it opens new gaps
- ✓ Fit AI into transaction monitoring, AML/CFT screening and Travel Rule information-sharing
- ✓ Know which wallet, custody and on-chain risks AI can surface and which it will quietly miss
- ✓ Recognise when an AI alert — or the absence of one — should not be trusted on its own
- ✓ Evidence to a regulator that your AI-assisted controls are sound and properly overseen
- ✓ Map each AI tool to the risk it covers and the human check that backs it

Curriculum

01 Where AI helps (and hurts) crypto compliance teams today

- Realistic uses of AI in crypto compliance: alert triage, screening, due-diligence support
- Where AI introduces new blind spots a rules-based system didn't have
- How generative AI tools fit (and don't) into a compliance workflow
- Separating capability from vendor overpromising in digital-asset tooling
- What stays a human judgement call regardless of the tool

02 AI in transaction monitoring, AML/CFT and the Travel Rule

- How AI-assisted monitoring differs from traditional rules and scenarios
- Using AI to triage and prioritise alerts without missing real risk
- Meeting the FATF Travel Rule: passing sender and recipient information with a transfer
- Screening, sanctions and customer due diligence in a digital-asset context
- How alerts feed suspicious-activity reporting and who stays accountable for it

03 Wallet, custody and on-chain risk that AI can and can't catch

- Blockchain-analytics basics: tracing flows and risk-scoring wallet addresses
- Crypto-specific risks: mixers, privacy coins, chain-hopping and pseudonymous wallets
- Custody and on-chain exposure risks that need human review
- What blockchain analytics and AI surface well, and where they fall short
- Combining on-chain signals with off-chain context for a real picture

04 Avoiding false confidence: when not to trust an AI alert

- Why a clean AI result is not proof that nothing is wrong
- How false positives and false negatives show up in crypto monitoring
- Building checks so analysts question, not rubber-stamp, AI output
- Recognising when a model is operating outside what it was built for
- Setting thresholds and overrides that keep humans in control

05 Showing your regulator that your AI controls are sound

- What 'explainable and overseen' means in a digital-asset compliance setting
- Evidence a supervisor expects: testing, monitoring and human oversight records
- Documenting why an AI-assisted control is fit for purpose
- Demonstrating that 'the system flagged it' is backed by real judgement
- Preparing for questions about how your AI tools actually work

06 A control map your compliance team can put to work immediately

- Building a map that links each AI tool to the risk it covers
- Recording the human check behind every automated step
- Identifying gaps where a risk has no clear control or owner
- Tailoring the control map to your exchange, custody or DeFi operations
- Keeping the map current as tools and typologies change

You keep

> An AI-in-compliance control map for your crypto operations.

Arthiq — live, in-person AI training for high-stakes teams.

Book a session: founders@arthiq.co · https://arthiq.co