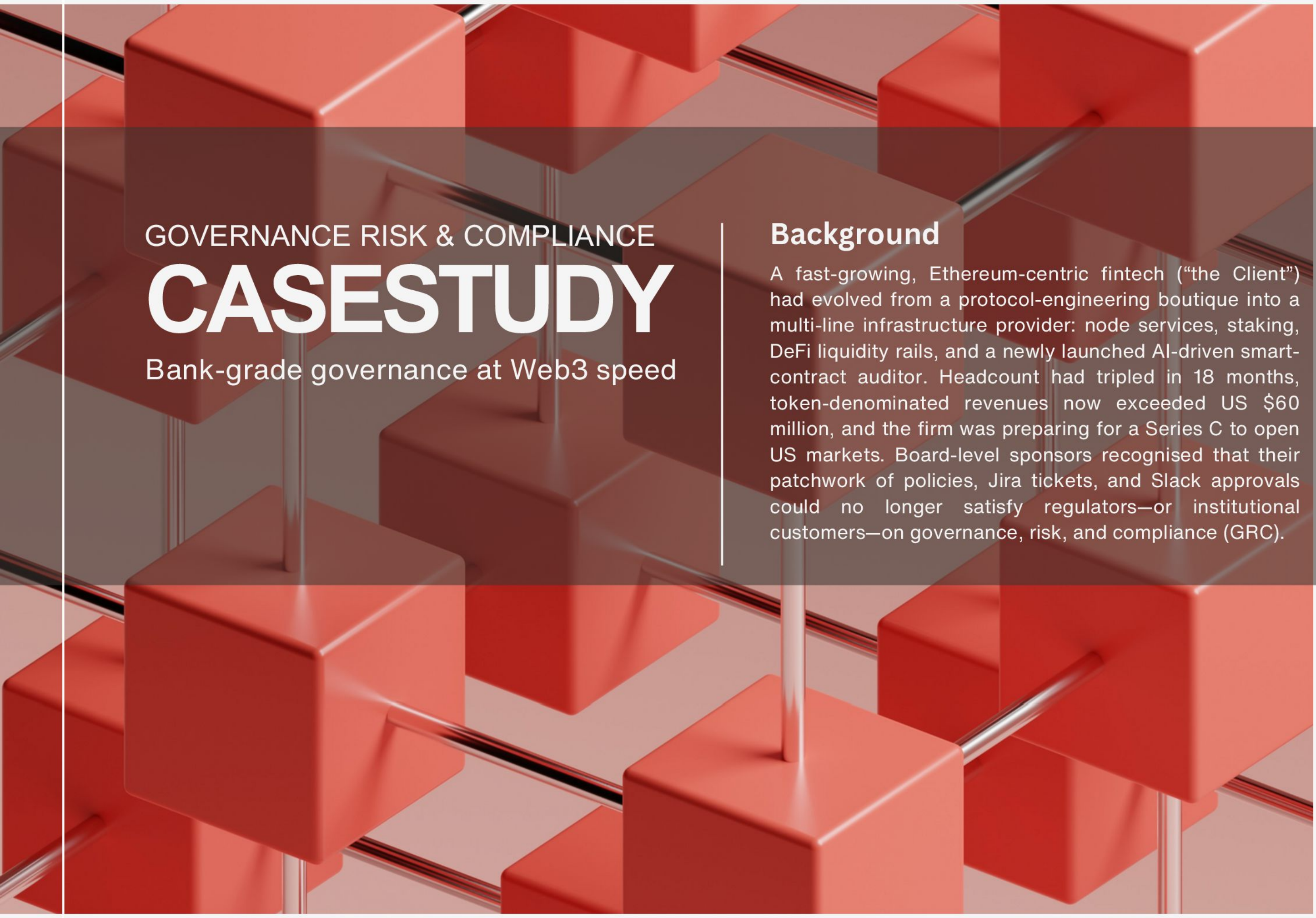
Enigma Risk Advisory Consulting



GOVERNANCE RISK & COMPLIANCE

CASESTUDY

Bank-grade governance at Web3 speed

Background

A fast-growing, Ethereum-centric fintech (“the Client”) had evolved from a protocol-engineering boutique into a multi-line infrastructure provider: node services, staking, DeFi liquidity rails, and a newly launched AI-driven smart-contract auditor. Headcount had tripled in 18 months, token-denominated revenues now exceeded US $60 million, and the firm was preparing for a Series C to open US markets. Board-level sponsors recognised that their patchwork of policies, Jira tickets, and Slack approvals could no longer satisfy regulators—or institutional customers—on governance, risk, and compliance (GRC).

Introduction

Enigma Risk Advisory was engaged to design and execute a future-proof GRC programme covering enterprise risk, information security, digital-asset custody, DeFi liquidity management, and AI/ML model governance. The mandate: deliver “bank-grade” controls without throttling developer velocity, and embed real-time transparency expected in decentralised ecosystems.

Challenges Faced

Theme	Pain Point	Strategic Implication
DeFi & Digital Assets	• 24/7 liquidity exposure • Cross-chain bridges • Impermanent-loss risk	Volatile capital buffers; unclear risk-ownership lines
Blockchain Operations	• Smart-contract releases shipped straight to mainnet • minimal segregation of duties	Elevated contract-failure, oracle-manipulation, and Extractable (MEV) risks
AI & ML	Rapid rollout of LLM-based auditor no model-risk policy no bias or hallucinaton KPIs	Legal liability for false-negative findings; upcoming EU AI Act
Regulatory Landscape	Simultaneous pursuit of Markets in Crypto-Assets Regulation (MiCA) (EU), Digital Asset Service Provider (DASP) (France), SOC 2 (US), ISO 27001 (global)	Audit-fatigue, duplicated evidence requests
Culture & Scale	Engineers allergic to paperwork; risk tooling scattered across GitHub, Notion, and Discord	Low control adherence and limited management

GOVERNANCE RISK & COMPLIANCE

CASESTUDY

Bank-grade governance at Web3 speed

Results and Impact

- 45% reduction in control-remediation cycle-time (from 22 days to 12) through automated evidence collection and risk-owner nudges.
- $8 million VaR compression on DeFi-treasury positions by deploying probabilistic stress tests and daily “liquidity at risk” dashboards.
- Zero critical audit findings in inaugural SOC 2 Type I attestation; ISO 27001 certification achieved 11 weeks ahead of target.
- AI model-risk framework adopted as board policy, enabling safe expansion of the auditor product and satisfying EU AI Act “systemic risk” provisions.
- Developer satisfaction +18 NPS points—controls embedded in existing Git workflows, not extra portals.

Solutions Implemented

a. Holistic GRC Architecture

- Single-pane cloud GRC platform (open-source core + custom API connectors) mapping 320 controls to ISO 27001, SOC 2, Markets in Crypto-Assets Regulation (MiCA), and internal risk taxonomies.
- Smart-contract control library: pre-commit hooks enforcing multi-sig approvals, gas-efficient audit tags, and automated differential testing.

b. Blockchain & DeFi Risk Engine

- On-chain telemetry ingestion via subgraphs and oracle feeds → real-time VaR, counter-party concentration, bridge risk scores.
- Scenario generator leveraging stochastic simulations for impermanent-loss and MEV shocks; outputs fed to treasury-rebalancing bot that writes trades to governance wallet.

c. AI/ML Model-Risk Governance

- Policy aligned to ECB Targeted Review of Internal Models (TRIM) and National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF).
- Four-line-of-defence model: product squads → risk science guild → Model-Risk Committee → board AI & Ethics sub-committee.
- Continuous-monitoring pipeline measuring hallucination rate, bias drift, and security exploitation vectors; results surfaced in Grafana and escalated via PagerDuty.

d. Culture & Operating Model

- “Risk-as-Code” workshops turned every Jira ticket into a control artefact; Slackbot “Sherlock” reminds owners 72 hours before attestations.
- Quarterly Risk Game-Days simulating bridge hacks and rogue-AI scenarios—integrated with chaos-engineering practice to hard-wire learning loops.

Conclusion

By fusing **quant-heavy DeFi analytics, blockchain-native controls, and enterprise-grade AI model governance** into a lightweight “risk-as-code” framework, the Client vaulted from start-up improvisation to top-quartile GRC maturity in under nine months.

The programme not only satisfied auditors and regulators but also unlocked capital efficiency, accelerated product launches, and bolstered the firm’s valuation narrative ahead of its Series C.

Most importantly, risk became a competitive differentiator—proof that disciplined governance can coexist with the pioneering spirit of Web3 and AI innovation.