

CASE STUDY

Continuous Assurance, Not Annual Attestation: How a Regulated Financial Services Firm Operationalised ISO 42001

Business Overview

Our customer is a regulated financial services organisation operating across retail and institutional markets, already managing an extensive compliance footprint spanning DORA, NIS2 and ISO 27001. As AI adoption accelerated across customer service, fraud detection and internal operations, the organisation moved to pursue ISO 42001 certification to formalise AI governance and satisfy both regulators and the board that AI-related risk was being actively managed – not just documented.

Pain Points / Challenges

01

No continuous, real-time visibility of AI-related controls across a complex, multi-framework compliance environment.

02

Manual evidence-gathering for audits and regulatory reviews was resource-intensive and prone to gaps between assessment cycles.

03

Board and regulator reporting relied on periodic snapshots rather than ongoing, verifiable assurance that controls were operating.

Business Challenges

With multiple overlapping regulatory frameworks already in place, the organisation was determined to avoid building a separate, siloed governance process for AI.

Existing assurance processes relied heavily on periodic, manual control testing, which was not well suited to the pace of change in AI tool adoption and regulatory expectations.



Multi-framework complexity: AI governance needed to sit alongside DORA, NIS2 and ISO 27001 controls, not duplicate or conflict with them.



Point-in-time assurance model: Annual and quarterly control testing left long gaps in which AI-related risk could go undetected.



Board and regulator expectations: Both the board and regulators expected continuous, evidenced assurance that AI governance was operating effectively, not a static framework document.



Audit fatigue across the three lines of defence: Control operators, risk and internal audit teams were spending significant time compiling manual evidence for each review cycle.

“Regulators and our own board expect us to prove, continuously, that AI governance is working — not describe it in a policy document once a year. We needed an assurance model that matched the pace of AI adoption, not the pace of our old audit cycle.”

Chief Risk Officer, Regulated Financial Services Firm

Our Solution

Quod Orbis mapped the organisation's ISO 42001 control requirements directly onto its existing DORA, NIS2 and ISO 27001 control environment, avoiding duplication and ensuring AI governance was embedded within the organisation's established risk framework rather than run as a separate initiative.

The CCM platform was deployed to continuously monitor AI-related controls across the organisation's technology estate, automatically ingesting evidence from existing data sources and correlating it against the mapped control set. This gave control operators, risk and internal audit teams a shared, real-time view of control performance, while board and executive stakeholders received group-wide summaries and maturity tracking without needing to interpret raw control data themselves.

The Results



Continuous, Real-Time Assurance

AI-related controls are now monitored continuously rather than assessed on a periodic, point-in-time basis.



Significant Reduction in Manual Testing Effort

Automated evidence collection substantially reduced time spent on manual control testing across the three lines of defence.



Unified Multi-Framework View

ISO 42001 controls are mapped alongside DORA, NIS2 and ISO 27001, giving one consolidated view instead of siloed assessments.



Board-Ready Reporting

Group-wide summaries and maturity tracking give the board and executive team ongoing visibility without technical translation.



Reduced Regulatory and Audit Fatigue

Immutable, continuously generated evidence is available on demand for regulators and auditors, reducing pre-audit scramble.



Improved Control Maturity Tracking

The organisation can now track the maturity of its AI governance controls over time, identifying areas requiring focus before they become issues.

Get in Touch

To find out how Quod Orbis can help your organisation embed ISO 42001 into an existing regulatory control environment with continuous, evidenced assurance, get in touch with our team.

Contact@quodorbis.com