CYBER MANAGEMENT ALLIANCE

INDEPENDENT ASSURANCE · ARTICLE-LEVEL EVIDENCE

Regulatory Alignment **and Policy Review**

Your policies, benchmarked clause by clause against FCA rules, DORA and the regulatory requirements that govern your firm.

- A precise, evidence-backed view of where your policies meet or fall short of applicable requirements
- Article-by-article mapping to DORA, FCA/PRA expectations and relevant supporting standards
- A priority-rated remediation tracker ready to support self-assessments, board reporting and supervisory scrutiny
- Forward-looking visibility of incident and third-party reporting requirements applying from 18 March 2027

For FCA-authorised firms, financial institutions, CISOs, risk and compliance leaders, COOs, boards and senior managers accountable for the control environment.

Prepared before · Effective during · Stronger after

PRACTITIONER-LED REGULATORY REVIEW

THE CHALLENGE

For regulated firms, policies are not paperwork. They are regulatory evidence.

Your policies are read by supervisors, requested by auditors and customers, and relied upon when senior managers must demonstrate that risks are properly governed. Yet many policy suites were written before today's requirements existed. Management-body approvals are unclear, review cycles have lapsed, responsibilities are inconsistent, and incident or supplier policies do not reflect the obligations they are meant to support.

DORA sets detailed expectations for ICT security policy content. The FCA expects operational resilience documentation to be substantive and current. From **18 March 2027**, new operational incident and material third-party reporting rules raise the bar again. The Regulatory Alignment and Policy Review identifies exactly where your policies stand against those expectations — before the question comes from your board, auditor or regulator.

WHAT IT IS

Regulatory assurance, article by article

A Regulatory Alignment and Policy Review is an independent, structured evaluation of your IT and information security policy suite against the specific regulatory instruments applicable to your firm. The review leads with FCA and PRA expectations, DORA and its ICT risk-management technical standard — Commission Delegated Regulation (EU) 2024/1774 — then applies relevant supporting benchmarks such as ISO/IEC 27001:2022, NCSC guidance, the NCSC Cyber Assessment Framework and UK data-protection requirements.

Every finding cites the relevant regulatory article, rule or standard clause and the exact section, paragraph or page in your document. Strengths are credited with the same rigour as gaps, creating a balanced and defensible record of your control environment. For UK-only firms without direct DORA obligations, DORA can be applied transparently as a benchmark baseline — not presented as an automatic legal requirement.

The result is an **article-mapped findings tracker** that supports your regulatory evidence pack, operational resilience self-assessment and remediation programme.

HOW IT WORKS

One regulatory perimeter. One review. One defensible record.

1 **Regulatory scoping**
We establish your FCA permissions, PRA status, DORA exposure, group structure, relevant obligations and the policy documents in scope.

2 **Clause-by-clause benchmarking**
Our practitioners review each policy against applicable DORA provisions, FCA/PRA expectations and supporting standards, while checking consistency across the suite.

3 **Article-level findings**
Every observation includes an exact document locator, the relevant article or rule, a plain-English explanation, a High/Medium/Low priority and a practical wording-level fix. Strengths are formally credited.

4 **Tracker delivery and walkthrough**
You receive one review sheet per policy, a summary dashboard and an Open/WIP/Closed/N/A status tracker. We walk your compliance and IT leads through the material findings.

5 **Closure and re-review**
A follow-up review can confirm remediation against the same requirements, creating a dated assurance trail for your board, auditor and supervisor.

WHAT MAKES IT DIFFERENT

Built for regulatory scrutiny, not generic box-ticking

Article-level precision
Findings reference the exact DORA provision, FCA/PRA expectation or standard clause that applies.

Forward-looking assurance
Incident, escalation and supplier policies are checked against requirements applying from 18 March 2027.

Senior-manager relevance
Governance gaps, unclear ownership and missing approvals are surfaced for accountable leaders.

One review, multiple uses
A balanced, low-disruption evidence base supports DORA documentation, FCA self-assessments, board oversight and due diligence.

WHAT YOU RECEIVE

A supervisory-ready regulatory evidence pack

Each Regulatory Alignment and Policy Review delivers:

- Article-level mapping to applicable DORA provisions, FCA/PRA expectations and supporting standards
- Exact document locations for every finding, down to section, paragraph or page
- High/Medium/Low priority ratings and practical wording-level remediation
- Independent recognition of policy strengths that meet or exceed the benchmark
- Suite-level findings covering contradictions, inconsistent governance and broken cross-references
- Forward-looking flags for operational incident and material third-party reporting requirements
- A summary dashboard showing findings by policy and priority
- A living Open/WIP/Closed/N/A tracker to evidence ownership, remediation and closure
- A findings walkthrough and optional re-review to demonstrate progress

Every finding is tied to a **specific article and an exact location** in your document — so remediation, board reporting and supervisory responses all point to the same defensible evidence.

Companion assessments

The Operational Resilience Assessment and Technical Resilience Assessment can validate whether the capabilities described in your policies work in practice.

The review provides independent assurance and regulatory relevance mapping; it is not legal advice, a compliance certification or a formal legal opinion.

SAMPLE OUTPUT

What article-level findings look like

NEXT STEPS

Ready to know exactly where you stand — **article by article?**

A regulated firm's policies should do more than exist. They should demonstrate clear ownership, current governance and alignment with the requirements that actually apply.

The Regulatory Alignment and Policy Review replaces generic reassurance with precise, independent evidence: what meets the benchmark, what falls short and what to fix before scrutiny intensifies.

It starts with a short scoping call. We map your regulatory perimeter, agree the policies in scope and define the benchmarks that matter to your firm.

Book a regulatory scoping call

Request the full review outline

Speak to our regulatory assurance team

One document-based review. One article-mapped tracker. **One defensible assurance record.**

CYBER MANAGEMENT ALLIANCE

+44 (0) 203 189 1422
info@cm-alliance.com
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ