

AI Governance

Practical and proportionate AI governance for regulated firms

“

Governance measures should be put in place to ensure effective oversight of the supply and use of AI systems, with clear lines of accountability established across the AI life cycle.

FINANCIAL CONDUCT AUTHORITY (FCA)

”

WHAT WE OFFER:



Independent AI Governance Reviews



Introduction of Control Framework



On-going support to maintain AI control



AI Data Governance

The Governance Reality

AI is already active within your business - in compliance, operations, and decision-making. Governance has not kept pace.

The challenge is not creating new layers of governance. It is ensuring existing governance frameworks adequately address AI-related risks and can be evidenced to regulators, investors and stakeholders without creating unnecessary operational burden.

Across regulated firms we consistently see:

- No central AI inventory
- Shadow use of tools such as ChatGPT and Copilot
- Unclear SM&CR accountability
- Third-party AI tools not subject to structured due diligence
- Governance frameworks that describe principles but fail to translate into operational controls
- Limited ability to evidence appropriate controls to regulators or investors



What Regulators Expect

The FCA's position is clear: existing obligations under SYSC, SM&CR, MAR, and the Consumer Duty apply in full to AI. The EU AI Act adds further requirements for EEA-active firms; the SEC framework applies in the US.

Firms are expected to evidence:

- A documented inventory of AI use across the firm
- Defined ownership and accountability under SM&CR
- Appropriate controls and oversight
- Effective management of third-party AI risk
- Audit trails that demonstrate governance in practice

AI Governance Self-Test



- Do we have a complete inventory of AI use across the firm?
- Could we explain how AI outputs are governed?
- Is accountability defined across senior management?
- Do first-line teams know what they can and cannot do with AI?
- Can second-line functions challenge AI use effectively?
- Would we be comfortable evidencing this to the FCA tomorrow?

If you cannot answer positively, a governance gap already exists - whether identified or not.



AI governance does not require entirely new governance structures. The challenge is ensuring existing governance, risk and compliance arrangements appropriately capture AI-related risks and decision-making.

Two Structural Gaps Every Regulated Firm Faces



Capability Gap

Oversight functions lack the tools and understanding to govern AI effectively.



Implementation Gap

No clear, consistent method to translate regulatory expectations into operational governance.

The Blueprint Solution



Explore how Blueprint's extensive expertise can provide the answer. Choose or combine from the following Blueprint GRC services:

1

AI GOVERNANCE REVIEW



Independent gap analysis of current AI usage controls. Formal report with prioritised recommendations.

2

FRAMEWORK IMPLEMENTATION



Full deployment of policies, risk assessments, use case register, approval workflows, and oversight structures.

3

ONGOING OVERSIGHT SERVICE



Retained monitoring regulatory updates, periodic reviews, and management information reporting.

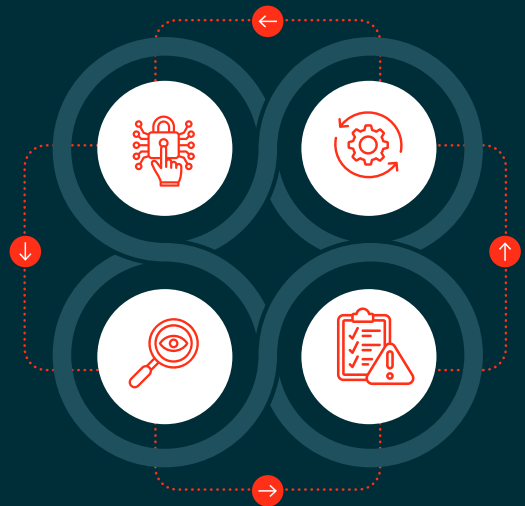
4

AI DATA GOVERNANCE



Bespoke programme focused on data classification, clean-up, and governance of data used within AI models.

The Framework: Four Core Areas



Blueprint GRC's approach is built around four interlocking areas, designed to translate high-level obligations into day-to-day operational governance:

1

AI CONTROL FRAMEWORK

Policy and Acceptable Use Standard

2

AI USE CASE LIFECYCLE

Governance and approval model

3

RISK ASSESSMENT FRAMEWORK

Know Your Needs, model assessment, risk tiering

4

OVERSIGHT & MONITORING

Vendor due diligence, use case register, MI reporting



Our **AI Governance solutions** provide:

- **Clarity** over complexity and implementation over theory
- **Evidence** over policy and monitoring over assumption
- **Assurance** in front of regulators
- **Practical** and proportionate governance tailored to the firm's AI use cases.

Three Lines of **Defence:**

1. Business and technology teams identify use cases, operate controls, own day-to-day risk, and maintain documentation.
2. Risk, compliance, and legal functions set standards, review higher-risk cases, and oversee whether controls remain effective.
3. Internal audit - or a suitably independent outsourced arrangement - provides impartial assurance that controls are designed and operating effectively.

Who this is for:

- FCA regulated firms, subject to FCA/PRA scrutiny
- Firms with EU and US regulatory nexus where other AI legislation exists
- Businesses in other sectors seeking to introduce or strengthen existing AI governance

If you couldn't answer the self-test with confidence, the gap is already there. **Let's close it.**

Why Blueprint GRC

The right blend of expertise,
experience, and insight

Meeting needs. Exceeding expectations.

Members of our team were former regulators, and all have worked in the Compliance Officer role, in-house, or as consultants for many years. This expertise is augmented by colleagues experienced in operations and data management.

We understand the expectations of the regulators – their approach to ‘supervising’ AI Governance is true to form and we can draw a line from first principles to evidential requirements necessary during a regulatory examination.

From an impartial review to benchmark your AI Governance, to a full framework implementation, we can help you evidence your controls are effective.

We help firms:

- Identify and govern AI use.
- Integrate AI governance into existing frameworks.
- Establish internal reporting and accountability.
- Evidence effective governance to regulators and stakeholders.
- Maintain oversight as AI use evolves.

Blueprint GRC delivers:

- AI Governance review and advice
- FCA and SEC regulatory support
- Outsourced GRC functions
- Fractional compliance resources
- Local and international regulatory reporting
- GIPS® and Performance analytics/marketing
- Operational support and data management
- Sanction screening



info@blueprintgrc.com | www.blueprintgrc.com

Blueprint GRC Limited

Registered Office:
5th Floor, 3 Dorset Rise,
London, EC4Y 8EN, UK

Blueprint GRC (EU) Limited

Registered Office:
171 Old Bakery Street
Valetta VLT 1455, Malta

Blueprint GRC (Performance), LLC

Registered Office:
8 The Green, Suite A, Dover,
Delaware, 19901, USA

