

 WHITE PAPER

Governing generative AI in UK financial services: a practical framework

A practical framework for regulated firms: the regulatory landscape, seven building blocks of AI governance, a maturity view and a 90-day plan.

Dutira editorial team  25 October 2026  11 min read

KEY TAKEAWAYS

- UK regulators are applying existing frameworks to AI rather than writing new rules. The task for firms is to show how their current obligations are met when AI is used.
- The biggest gap in most firms is not the models data teams build, but everyday generative AI used by employees.
- Seven building blocks — policy, inventory, risk assessment, controls, people, oversight and monitoring, evidence — give a framework proportionate to any size of firm.
- Governance that runs inside everyday work produces evidence as a by-product. Governance that runs beside it produces paperwork.

Executive summary

Generative AI has arrived in UK financial services faster than most governance frameworks were designed to handle. Employees use it to draft, summarise, research and code. Vendors are building it into the software firms already use. And a growing number of firms are deploying it in customer-facing processes.

The regulatory position is clear in outline. The Financial Conduct Authority has said it does not plan to introduce AI-specific rules and relies on existing frameworks — notably the Consumer Duty and senior manager accountability. In October 2026 it published observations of good practice and areas for improvement, with illustrative case studies. The expectation is not that firms comply with a new AI rulebook, but that they can show how their existing obligations are met when AI is involved.

This paper sets out a practical framework for doing that. It is written for chief compliance officers, chief risk officers, heads of technology and the senior managers accountable for how AI is used. It covers:

1. The regulatory landscape for AI in UK financial services.
2. Why everyday generative AI is the governance gap most firms have not closed.
3. Seven building blocks of AI governance.
4. A maturity view to help firms decide where to focus.
5. A 90-day plan.
6. A checklist for boards and senior managers.

This paper is general information, not legal or regulatory advice. Which rules apply to a firm depends on its permissions, business model and regulatory status.

1. The regulatory landscape

The FCA's approach

The FCA's statement [AI and the FCA: our approach](#) describes a principles-based, outcomes-focused approach. The FCA says it does not plan to introduce extra regulations for AI, relying instead on existing frameworks, and it names the Consumer Duty and the accountability of senior managers under SM&CR as particularly relevant.

Two developments in 2026 add detail:

- **AI Live Testing.** In April 2026 the FCA announced the [second cohort](#) of AI Live Testing, which helps firms explore risk management and live monitoring for AI deployment. Testing runs to the end of 2026 and an evaluation report is expected in the first quarter of 2027. Participation is not described as approval.
- **Good practice and areas for improvement.** In October 2026 the FCA published [AI in financial services: good practice and areas for improvement](#). The FCA describes the examples as illustrative and non-exhaustive and says they do not create new requirements. Its themes include structured challenge and sign-off before deployment, simple risk tiers that intensify testing and monitoring, a central inventory of AI with owners, mapping AI responsibilities across senior managers, human oversight decided by risk assessment, forward-looking monitoring with thresholds and audit trails, role-specific training, and avoiding single-provider dependence.

The existing frameworks that apply

The following parts of the FCA Handbook are the most commonly relevant. Scope varies by firm, and each firm should record its own applicability decisions.

Framework	Relevance to AI
Principles for Businesses ↗	Principles 2 (skill, care and diligence), 3 (management and control) and 11 (relations with regulators) apply to every authorised firm.
SYSC 4.1 ↗	Robust governance: clear responsibilities, risk management and internal controls — including for AI.
SYSC 8 ↗	Outsourcing, relevant where AI services are provided by third parties. Addressed to common platform firms; others apply it as guidance.
SYSC 9.1 ↗	Record-keeping: orderly records of the business and internal organisation.
SYSC 15A ↗	Operational resilience for in-scope firms, including mapping the resources — such as AI services — that support important business services.
SYSC 24–27 ↗ and COCON ↗	SM&CR: allocation of responsibilities, certification and the individual conduct rules.
PRIN 2A — Consumer Duty ↗	Retail market business: outcomes for products and services, price and value, consumer understanding and consumer support, wherever AI is used.
SUP 15.3 ↗	Notifications to the FCA, read with Principle 11 — relevant when an AI incident may be significant.

FCA guidance also remains relevant, including the Consumer Duty guidance [FG22/5](#) ↗ (on which the FCA has consulted on a replacement) and the guidance on [vulnerable customers, FG21/1](#) ↗.

Data protection

Where AI processes personal data, [UK GDPR](#) ↗ applies and the Information Commissioner’s Office is the regulator. The ICO’s [guidance on AI and data protection](#) ↗ covers lawful basis, fairness, transparency, data minimisation, security and individual rights, and says AI processing of personal data will

usually need a data protection impact assessment. The Data (Use and Access) Act 2025 substituted the provisions on automated decision-making; firms should check which provisions are in force.

Other regimes

Firms with prudential regulation by the PRA, or with operations in the European Union, will have further expectations to consider — for example on model risk management, or under the EU's AI Act, which applies in phases. These are outside the scope of this paper; firms should take advice on their position.

2. The everyday AI gap

Most early AI governance work in financial services focused on models: credit scoring, fraud detection, pricing, trading. These are important, usually well understood, and often already subject to model risk management.

The faster-growing exposure is different. It is general-purpose generative AI used by employees across the business:

- An adviser summarising meeting notes.
- A complaints handler drafting a response.
- A marketer writing a promotion.
- An operations analyst pasting a spreadsheet to “tidy it up”.

This use is:

- **Widespread** — it reaches every department, not a specialist team.
- **Often invisible** — much of it happens in browser tabs and personal accounts the firm has not approved (“shadow AI”).
- **Data-rich** — people paste exactly the documents that contain client information.
- **Close to customers** — drafts become letters, emails and promotions.
- **Poorly evidenced** — there is often no record of what was used, with what data, or who checked the output.

A governance framework that covers models but not everyday use leaves the largest door open. The framework below is designed to cover both.

3. Seven building blocks of AI governance

3.1 Policy

An AI acceptable use policy sets out which tools are approved, for what purposes, with which data, what needs approval, and how to report a concern. It should be short, specific, versioned and acknowledged by each person. See our guide to [writing an AI acceptable use policy](#).

What good looks like: a policy people can apply in the moment, with concrete examples; acknowledgements recorded against each version; a named owner and review date.

3.2 Inventory

A central register of AI use cases, each with an accountable owner, purpose, data, model or provider, customer impact, risk rating, controls, approval and review date. The register should include vendor AI features and everyday generative AI, not just in-house models. See [building an AI use case register](#).

What good looks like: the register is the single source for approvals, access, monitoring and reporting, and it is updated as part of how work happens — not once a year.

3.3 Risk assessment

A methodology that rates each use case on factors such as customer harm, Consumer Duty implications, accuracy and explainability, data sensitivity, autonomy and third-party dependence, and records how controls reduce inherent risk to residual risk. Simple tiers — low, medium, high, prohibited — determine how much testing, approval and monitoring each use case needs.

What good looks like: ratings with recorded rationale; independent review of assessments for higher tiers; reassessment when the use case, model or data

changes.

3.4 Controls

Controls translate policy into the path of every AI request:

- Which models each role may use.
- A data-classification ceiling for each model.
- Detection of client identifiers and confidential information, with masking, holding for approval or blocking.
- Approval before high-risk outputs are used or AI agents take actions.
- Checks on AI output before it is shown, where appropriate.

What good looks like: controls that act automatically, explain themselves to the user, are tested before changes go live, and are themselves tested periodically.

3.5 People

Role-based training for everyone who uses AI, with knowledge checks and records; specific training for reviewers on automation bias; and attestations, tied to policy versions, that let people declare exceptions rather than forcing a blanket confirmation. See [AI training for staff](#).

What good looks like: completion and understanding evidenced by role; declared exceptions followed up without penalising honesty.

3.6 Oversight and monitoring

Human review where the risk assessment says it is needed, designed to be meaningful: reviewers see the content, use a checklist, record a reason, and duties are separated. Monitoring of AI activity and outcomes against thresholds, with alerts, investigation cases and incident management, including confidential and speak-up routes. See [human oversight of AI](#).

What good looks like: oversight quality is itself measured (for example, implausibly fast approvals are flagged); monitoring leads to action.

3.7 Evidence and management information

Records of decisions, approvals, attestations, incidents and control tests, kept in a way that shows they have not been altered; regular management information for senior managers and the board; and the ability to export evidence for internal audit or a regulator request.

What good looks like: evidence produced by everyday operation; management information that shows trends and exceptions; senior management reviews with recorded challenge. No single “compliance score” — a score hides exactly the detail a board needs.

Accountability across the blocks

Under SM&CR, the firm decides how AI responsibilities are allocated. A common model gives one senior manager ownership of the AI governance framework, with each business line’s senior manager accountable for AI used in their area. Whatever the model, it should be documented, reflected in statements of responsibilities, and supported by the management information each senior manager needs to take reasonable steps. See [SM&CR and AI](#).

4. A maturity view

Firms are at different starting points. The table below describes three broad stages for each building block. It is a way to decide where to focus, not a scale to score against.

Building block	Foundational	Managed	Embedded
Policy	A published AI policy	Versioned, acknowledged by all staff	Linked to controls that apply it automatically
Inventory	A list of known AI uses	Owned register with risk ratings and review dates	Register drives approvals, access and reporting
Risk assessment	Informal judgement	Documented methodology and tiers	Independent review; reassessment on change
Controls	Policy reliance	Approved tools with some technical controls	Every request checked; controls tested
People	General awareness	Role-based training with knowledge checks	Attestations with exceptions followed up
Oversight and monitoring	Ad hoc review	Defined review points and monitoring	Oversight quality measured; thresholds and alerts
Evidence	Documents on request	Central records	Tamper-evident records; regular MI and reviews

Most firms will find they are at different stages for different blocks. The highest-value moves are usually the ones that close the everyday AI gap: an approved route for staff, controls in the path of each request, and a register that captures what is really happening.

5. A 90-day plan

Days 1–30: understand and stabilise

- Run a discovery exercise: surveys, team conversations, network and expense data. Record every AI use found.
- Publish an interim AI acceptable use policy and collect acknowledgements.
- Decide who owns the AI governance framework at senior manager level, and document it.
- Agree the risk tiers and the minimum controls for each tier.

Days 31–60: provide an approved route and controls

- Make an approved AI tool available to staff, with model access by role, data ceilings and sensitive-data detection.
- Move the highest-risk uses through formal assessment and approval.
- Launch role-based training with knowledge checks.
- Set up an incident route, including a confidential option.

Days 61–90: monitor, evidence and report

- Start monitoring AI activity against agreed thresholds.
- Run the first attestation cycle, allowing exceptions, and follow them up.
- Produce the first AI management information pack for senior managers and the board.
- Schedule reviews for each use case and provider, and plan the first control tests.

6. Checklist for boards and senior managers

1. Do we know where AI is used across the firm, including by employees using general-purpose tools?

2. Who is accountable for the AI governance framework, and for AI in each business area?
3. What is our risk appetite for AI, and which uses are outside it?
4. Do employees have an approved AI tool, and do controls stop restricted data reaching AI services?
5. Which AI outputs reach customers, and where does a person review them?
6. How do we know staff understand the AI policy, and what exceptions have they declared?
7. What do we monitor, against which thresholds, and what happened when thresholds were breached?
8. Which third parties do our AI uses depend on, and what is our plan if one fails or changes?
9. Could we produce evidence of all of this for internal audit or a regulator request tomorrow?
10. When did we last review this, and what changed as a result?

Conclusion

AI governance in UK financial services is less about new rules than about applying existing ones to a technology that is used everywhere, changes quickly and is easy to use invisibly. Firms that put governance inside everyday work — an approved tool, controls on every request, a live register, honest attestations and evidence produced as a by-product — will find it easier to use AI well and easier to show they are doing so.

If you would like a quick view of where your firm stands, the [AI governance readiness assessment](#) takes about three minutes. It is a self-assessment, not a certification.

About Dutira

Dutira is an AI compliance and governance platform for regulated businesses. It gives employees access to approved AI models while compliance teams control policies, monitor usage and maintain audit-ready evidence. Dutira is an independent technology solution designed to support AI governance and

oversight. It is not affiliated with, endorsed by or approved by the Financial Conduct Authority, and use of the platform does not guarantee regulatory compliance.

SOURCES

[FCA — AI and the FCA: our approach ↗](#)

[FCA — AI in financial services: good practice and areas for improvement \(October 2026\) ↗](#)

[FCA — second cohort for AI Live Testing \(April 2026\) ↗](#)

[FCA Handbook — PRIN 2.1 The Principles for Businesses ↗](#)

[FCA Handbook — SYSC 4.1 General organisational requirements ↗](#)

[FCA Handbook — SYSC 8 Outsourcing ↗](#)

[FCA Handbook — SYSC 9.1 Record-keeping ↗](#)

[FCA Handbook — SYSC 15A Operational resilience ↗](#)

[FCA Handbook — SYSC 24 Allocation of prescribed responsibilities ↗](#)

[FCA Handbook — COCON Code of Conduct ↗](#)

[FCA Handbook — PRIN 2A The Consumer Duty ↗](#)

[FCA — FG22/5 Final non-Handbook guidance on the Consumer Duty ↗](#)

[FCA — FG21/1 Fair treatment of vulnerable customers ↗](#)

[FCA Handbook — SUP 15.3 General notification requirements ↗](#)

[ICO — Guidance on AI and data protection ↗](#)

[UK GDPR \(legislation.gov.uk\) ↗](#)

General information, not legal or regulatory advice. Which rules apply depends on your firm's permissions, business model and regulatory status; check the sources for the current text. Last reviewed 25 October 2026. Dutira is not affiliated with, endorsed by or approved by the Financial Conduct Authority.