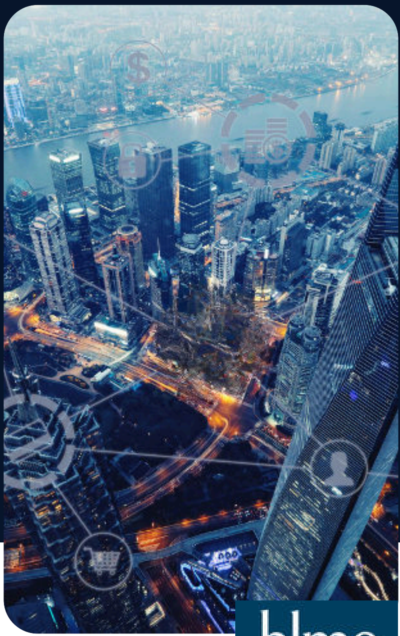

Pathfinder
IT, Data & Cybersecurity

Case Study

Embedding AI governance controls in a banking environment

BLME, a UK-based Islamic bank operating to Sharia principles was in need of support to develop a practical AI governance framework across the UK, Dubai and Jersey.

Context

As part of a wider data protection and governance engagement, the bank needed to develop a responsible and evidence-based approach to AI adoption within a regulated financial services environment.

Pathfinder assessed the bank's emerging AI governance framework, challenged draft policy content, identified gaps in the AI strategy and tested whether proposed commitments were practical, proportionate and capable of being evidenced.

Challenge

The key challenge was to ensure that AI governance was not treated as a technology workstream, but as a cross-functional risk issue involving data protection, IT security, legal, operational risk, business ownership and executive oversight.

This cross-functional approach was essential to secure strong stakeholder buy-in and make the governance model workable.

The Approach

Pathfinder brought a practical, implementation perspective to the bank's AI governance discussions. The focus was on helping the bank move from broad responsible-AI principles towards a more workable governance model.

We challenged areas where commitments appeared ambitious but not yet supported by defined processes, accountable owners, or key evidence requirements.

This included questions around:

- AI risk assessment, including DPIA screening for AI tool onboarding
- Acceptable residual risk
- Transparency
- Content authentication
- Monitoring of misuse, intended use and policy deviation

Pathfinder also revised the DPIA process so AI-specific risk factors were captured during the onboarding of new tools and use cases.

Pathfinder clarified the distinction between advisory, assurance and operational responsibilities and showed the bank that AI governance would need to connect with existing policies and controls (such as those covering third-party management and risk management) rather than sit in isolation.

"... Pathfinder approached complex issues professionally and reliably, particularly where legal, technology, IT security and governance considerations needed to come together. They worked well with stakeholders, communicated clearly and brought a ***pragmatic style*** *that helped move the work forward and get things done.*

I particularly valued their contribution on data protection matters requiring close collaboration with the Bank's IT and Security teams, as well as its constructive input into the Bank's AI Working Group on governance and policy matters..."

Paul Coomber
Head of IT & Security
Bank of London & The Middle East

The Value Added

Pathfinder helped the bank strengthen its AI governance approach by making it more **practical, proportionate and aligned** to the realities of a regulated banking environment.

We shifted the discussion from high-level AI principles to **practical questions** senior stakeholders need answered: *who owns the risk, how is the control performed, and how is it possible to evidence that the process is working?*

With the bank benefiting from independent challenge across data protection, IT/security and governance considerations, they had a defendable foundation for AI adoption.

The Result: an AI framework that was clear and credible, and a governance model better able to support innovation while managing privacy, security, operational and regulatory risk.

Pathfinder Delivered:

- **AI Governance:** We broadened the bank's AI governance approach to take a data protection, governance and operational risk perspective and challenged commitments where ownership, actions, controls or delivery plans were not yet clear.

- **Roles, Responsibilities & Accountabilities:** We widened the range of key stakeholders in the AI governance framework to include legal, data protection and third-party management, ensuring their needs of an AI governance framework were included.

- **Escalation & Governance Alignment:** Existing escalation routes between the bank's AI Working Group and its risk management committees were improved, so AI risks could be managed with the minimum of delay.

- **Embedded AI Governance Controls:** Pathfinder helped BLME to assess new AI tools within the bank's wider control framework, including DPIAs, risk management, vulnerability management, data protection, information security and third-party oversight

Pathfinder helped BLME turn AI governance from a policy concept into a practical operating framework.

Paul Coomber
Head of IT & Security
Bank of London & The Middle East

*"...We had the pleasure of working with **Pathfinder** during its engagement supporting BLME, and I would have no hesitation in recommending them. They brought a strong combination of data protection expertise, sound judgement and a clear focus on what is practical in a regulated banking environment...*

***Pathfinder** is exactly the kind of consultancy you would want involved: knowledgeable, measured, collaborative and focused on delivering the right outcome."*

pathfinderpm.co.uk

Find the right path to safe AI integration for your business

Contact:

+44 (0)20 3143 5558
info@pathfinderpm.co.uk
London, UK

Pathfinder
IT, Data & Cybersecurity