INTERNATIONAL AI IN FINANCIAL SERVICES REVIEW 2025 / 26

Beaumont Capital Markets
www.beaumont-capitalmarkets.co.uk

UAE

Deploying AI in Financial Institutions – Legal and Governance Best Practices

GIBSON DUNN

Sameera Kimatrai
Counsel

skimatrai@gibsondunn.com

+971 4 318 4616

www.gibsondunn.com

BIO

Sameera Kimatrai is an English law qualified of counsel in the Dubai office of Gibson, Dunn & Crutcher and a member of the firm's Financial Regulatory Practice Group. She has experience advising governments, regulators and a broad range of financial institutions in the UAE including investment managers, commercial and investment banks, payment service providers and digital asset service providers on complex regulatory issues both in onshore UAE and in the financial free zones. Sameera has particular experience in digital asset regulation across the Middle East and Africa having spent time as a senior regulatory lawyer in the legal department of a large digital assets exchange.

Sameera has been recognized as a Rising Star by The Legal 500 Middle East for Financial Services Regulation. She has also been ranked in Chambers and Partners for FinTech Legal in United Arab Emirates.

GIBSON DUNN

GIBSON DUNN

BIO

Aliya Padhani is an English law qualified Associate in the Dubai office of Gibson, Dunn & Crutcher and a member of the firm's Financial Regulatory Practice Group. She has experience advising governments, regulators and a broad range of financial institutions in both the UAE and UK, including investment managers, commercial and investment banks, payment service providers, FinTechs and digital asset service providers on complex regulatory issues.

Aliya Padhani
Associate

apadhani@gibsondunn.com

+971 4 318 4625

www.gibsondunn.com

GIBSON DUNN

1. Introduction

Artificial Intelligence (AI) is now a core part of organisational strategy, moving rapidly from experimental use to mainstream deployment. Across industries, particularly in financial institutions and the rapidly evolving fintech sector, AI is being deployed to accelerate processes, improve accuracy, and generate efficiencies at a scale that human-only operations cannot match. From automating complex compliance tasks to enhancing fraud detection, facilitating customer onboarding, and data analysis, these tools are reshaping how organisations operate.

This transformation, however, is happening at extraordinary speed, and largely in the absence of prescriptive regulation. In most jurisdictions, including the United Arab Emirates, regulators have so far adopted a cautious, “wait and see” approach: issuing soft guidance, piloting charters, and observing developments in peer markets before enacting hard law. This reflects a delicate policy balancing act – one which looks to encourage innovation and technological advancements whilst seeking to guard against some of the very real risks these systems can pose. The result is a regulatory gap, where the pace of adoption has outstripped the evolution of binding legal frameworks.

> “
>
> AI is transforming industries, but in the absence of clear regulation, organisations must self-regulate to ensure safe, fair, and transparent deployment.

In this environment, the responsibility for ensuring that AI is deployed safely, fairly, and responsibly has shifted onto the shoulders of organizations themselves as regulators look to impose self-regulation through open-source toolkits to enable the responsible use of AI in the financial industry. In this self-regulatory environment, Boards and senior management cannot afford to treat AI as just another operational upgrade. The governance of these tools demands active oversight, informed scrutiny, and alignment with a clear set of principles that safeguard legal compliance, ethical integrity, and consumer trust.

As the risks of ungoverned AI become more visible, from biased outcomes and opaque decision-making to breaches of privacy, organizations must learn to self-regulate. This means critically assessing not only whether to adopt AI tools, but how to deploy them in ways that embed core principles such as fairness, transparency, accountability, and human oversight from the outset.

The central question is therefore not whether AI will be used, but how it can be harnessed responsibly in the current climate of uncertainty. This requires the implementation of a governance framework that allows organisations to review AI tools against core principles, identify potential risks, and implement governance processes proportionate to the impact of each system. In the absence of clear statutory mandates, such internal frameworks are increasingly important and must be grounded in sustainable, legally defensible, and socially responsible AI adoption.

2. Core Legal and Ethical Principles for AI Governance

As organisations increasingly turn to AI tools to enhance efficiency and streamline internal processes, they must do so with a clear understanding of the legal and ethical implications of using these tools.

There is a growing consensus that effective AI governance is essential, supported by a framework of clear principles to ensure these tools are deployed safely, fairly, and in a manner that inspires consumer trust.

The following principles should be considered by organisations when designing governance frameworks and screening their AI tools to ensure responsible deployment:

- **Human Responsibility and Oversight** – Human-in-the-Loop AI addresses the need for human oversight and accountability. Unlike fully autonomous AI systems that operate without human intervention, Human-in-the-Loop involves humans at critical stages - from data annotation to continuous feedback and decision-making. However sophisticated an AI tool may be, its outputs must be reviewed, interrogated, and validated by a human decision-maker. This is especially critical for high-impact determinations with legal or regulatory consequences, which should never be left solely to automation. This is crucial for highly regulated financial institutions where senior management are held accountable for decision making. Oversight over these AI tools must be substantive, not simply symbolic, ensuring that accountability remains traceable and enforceable at every stage.

- **Fairness** – Individuals and entities affected by AI-assisted outcomes and decisions should be given the opportunity to understand how those outcomes were reached and to challenge them where appropriate. Fairness also means preventing AI from reinforcing existing social or systemic biases. Achieving this requires continuous scrutiny of both algorithms and training datasets, with proactive measures to identify and correct discriminatory patterns.

- **Transparency** – The opacity of "black box" AI tools is fundamentally at odds with responsible governance. Organisations should favour systems with built-in explainability, which can document and articulate the reasoning behind interactions and outputs. Transparency must operate on two levels. Internally, organisations must ensure that all AI systems are understood by their users, with documented rationales for deployment, use cases, and limitations. Externally, parties impacted by AI-assisted decisions should be informed about the role of AI in those processes, with sufficient explanation to facilitate meaningful scrutiny.

- **Justifiability and Contestability** – AI systems must be auditable. Organisations must retain records that explain how and why AI tools reached specific conclusions, particularly where these conclusions form part of a broader decision-making process. Importantly, the use of AI must not diminish the rights of individuals to challenge decisions that affect them. Mechanisms for appeal or reconsideration must remain robust and accessible.

- **Safety and Integrity** – AI tools should undergo rigorous pre-deployment testing to validate their accuracy and reliability, followed by ongoing monitoring to detect errors, hallucinations, or behavioral drift. Strong vendor management processes are equally important, ensuring that third-party AI solutions meet the organisation's standards for performance, security, and compliance. Without these safeguards, organisations risk deploying tools that make flawed recommendations, causing reputational damage and potential legal liability.

- **Data Privacy and Confidentiality** – Given that AI systems often rely on large volumes of personal or sensitive data, strict compliance with data protection laws should be ensured. This includes not only the secure handling of data, but also minimising data use, ensuring lawful bases for processing, and honouring individuals' rights to access, correct, or delete their information.

> "
>
> Human-in-the-Loop AI ensures accountability by requiring human oversight at critical stages, maintaining transparency, fairness, and contestability in decision-making.

3. Implementing a Tiered AI Impact Framework

Not all AI tools present the same level of impact to an organisation or risk. Some may be limited to back-office process improvements with minimal external impact, while others may directly influence high-stakes decisions affecting consumers, regulatory compliance, or an organisation's core operations. For this reason, companies should adopt a tiered governance framework underpinned by a structured risk-scoring methodology. This involves assessing each AI tool against defined criteria, such as its potential to affect customer outcomes, create legal exposure, or disrupt critical business processes, and assigning it a risk rating. Tools with higher risk scores should be subject to more stringent oversight, testing, and documentation requirements, while lower-impact tools may require proportionately lighter controls. By applying a risk matrix in this way, organisations can ensure that AI governance is both proportionate and effective, allocating compliance resources where they are most needed and safeguarding both the organisation and the consumers it serves.

4. Practical Governance Recommendations

When deploying AI tools, organisations must approach governance as a core strategic function, not a peripheral compliance exercise. AI can deliver significant business value, but it also presents unique risks, operational, legal, reputational, and ethical, that demand proactive oversight. The following governance arrangements represent a best-practice approach, combining high-level principles with detailed operational measures.

A. Board and Senior Leadership Oversight

AI adoption decisions should not be confined to the technical or operational level. Senior leaders must be actively involved in the selection, approval, and strategic integration of AI tools, while boards should exercise formal oversight of AI governance frameworks. This includes regular briefings on the organisation's AI portfolio, key risks, and mitigation strategies. The Governing Body should explicitly approve all high-impact AI deployments and remain accountable for their outcomes.

Whether or not a company is currently using AI, it still faces strategic business risks in the emerging AI-driven economy. Boards must treat AI governance as a standing agenda item and ensure that organisational readiness, risk appetite, and ethical boundaries are clearly defined.

> “
>
> Effective AI governance requires active board oversight, a comprehensive framework, human-in-the-loop accountability, and rigorous vendor due diligence to manage risks and ensure ethical deployment.

B. Establish a Comprehensive AI Governance Framework

A documented AI governance framework should govern the entire lifecycle of AI tools - from concept and acquisition through to deployment and ongoing monitoring. This framework should:

- Define the roles and responsibilities of internal stakeholders (e.g., risk, compliance, data privacy, IT, and business units) and external vendors.

- Establish policies, procedures, standards, and controls tailored to AI, including requirements for transparency, explainability, and fairness.

- Incorporate change management protocols to ensure that updates to AI tools, such as model retraining or parameter adjustments, are tested, documented, and approved.

- Require pre-deployment validation (including bias, stress, and performance testing) and post-deployment monitoring to confirm continued compliance and reliability.

Include a risk scoring methodology to classify AI tools by potential impact on the organisation and its consumers, enabling proportionate oversight.
Be approved by the Governing Body and reviewed annually.

C. Mandate Human Oversight and Declarations

AI systems, especially those which are higher risk rated, must operate within a “human-in-the-loop” or “human-on-the-loop” framework. All AI-assisted processes should:

- Include a documented declaration of independent human review, confirming that outputs have been interrogated and validated.
- Assign named individuals with decision-making authority who remain accountable for the final outcome.
- Require escalation protocols for any AI outputs that fall outside predefined confidence or risk thresholds.

This not only reinforces accountability but also mitigates the risk of uncritical reliance on algorithmic results.

D. Vendor Screening and Tool Due Diligence

Before procuring AI tools or outsourcing AI-related services, organisations should conduct robust vendor due diligence. This should assess:

- **Materiality** of the service to the organisation's operations and risk profile.
- **Technical maturity** and track record of the vendor, including history of compliance breaches or security incidents.
- **Security controls** such as authentication, encryption, access management – it should be assessed whether these are comparable to or exceeding the organisation's internal standards.
- **Data location and sovereignty**, ensuring that storage and processing meet jurisdictional requirements (e.g., UAE data localisation or cross-border transfer restrictions).
- **Testing history** including vulnerability assessments, penetration testing, and performance benchmarks.
- **Adherence to recognised standards** and relevant sector-specific certifications.

Vendors of AI tools should also be required to provide transparency on their model architecture, training data provenance, and bias mitigation processes. The results of vendor due diligence should be documented and factored into the AI risk score.

E. Provide Training for AI Users

Training and awareness are critical to the responsible deployment of AI. An AI system can only be as effective, fair, and compliant as the people who operate and oversee it. Organisations must therefore implement comprehensive training programmes that go beyond technical functionality to address the legal, ethical, and reputational risks inherent in AI use. These programmes should also cover the cognitive biases that can distort human interpretation of AI outputs, ensuring that staff are equipped to question, challenge, and, where necessary, override AI-generated recommendations. Such training should be mandatory for all personnel involved in the deployment, monitoring, or decision-making processes linked to AI, with refresher courses provided periodically and whenever there are significant changes to AI systems or governance requirements.

F. Prioritise Explainability

A further cornerstone of effective AI governance is explainability. Organisations should avoid the use of opaque "black box" models in favour of systems that provide native explainability, such as detailed breakdowns of decision-making processes, including the weights or factors influencing an outcome, or that are supplemented with interpretability layers capable of translating complex outputs into clear, comprehensible explanations. This requirement applies both internally, to facilitate oversight and debugging, and externally, to ensure that individuals affected by AI-driven decisions have a meaningful understanding of how those decisions were reached.

G. Test and Benchmark Extensively

Rigorous testing, benchmarking, and ongoing monitoring are essential to ensuring the integrity and reliability of AI systems. Before deployment, tools should be tested against historical datasets to validate their accuracy, fairness, and compliance with relevant standards. Stress and load testing should confirm that the system can operate effectively under high-volume or atypical conditions. Once deployed, AI systems must be subject to continuous monitoring to detect issues such as model drift, anomalies, or a decline in accuracy. These controls should be complemented by scheduled and ad hoc audits to verify adherence to governance policies and regulatory obligations. All test results and audit findings should be documented and fed into a continuous improvement cycle.

H. Public Disclosure and Disclaimers

Transparency with stakeholders is equally vital. Organisations should openly disclose the use of AI in any decision-making processes that materially affect customers or the public, providing plain-language explanations of the AI's role, purpose, and limitations. For public-facing tools, clear disclaimers should state that AI-generated outputs are intended for informational purposes and do not replace professional judgment or official determinations.

I. Monitor and Audit Continuously

Governance is not a one-time event. Policies, risk scoring methodologies, and oversight mechanisms should evolve in response to shifts in the organisation's strategic priorities, changes in applicable legal and regulatory requirements, and advances in AI capabilities or industry best practices. Regular reviews should be undertaken to confirm that AI applications continue to produce fair, consistent, and ethical outcomes, and that they remain aligned with the organisation's broader values, ethical standards, and codes of conduct.

> "
>
> Vendors of AI tools should provide transparency on model architecture, training data, and bias mitigation to ensure accountable AI governance.

Conclusion

AI presents immense opportunities, but its power must be tempered by principled governance. For legal professionals and regulators, the path forward lies in building structures that respect the law, protect the consumer, and ultimately preserve human agency in decision-making.

In jurisdictions like the UAE, where AI is a national policy priority, the challenge is to harness its potential while embedding strong legal safeguards. AI, properly governed, can be a catalyst for progress. But without legal guardrails, it becomes a risk too great to ignore.