Shape the future with confidence

The future of AI compliance

The better the question.
The better the answer.
The better the world works.

Artificial Intelligence innovation in Financial Services: leverage existing Financial Conduct Authority (FCA) principles to promote ethical innovation and manage strategic risk

You should read this if you are responsible for AI Risk Management and Governance in the Financial Services sector.

Firms across Financial Services are increasingly integrating AI technologies into their operations. AI can be used to deliver huge cost-savings, new insights, new business models, and positive outcomes for consumers. Examples where AI is already having a positive impact include fraud detection, enhanced customer experience, anti-money laundering, product innovation and enhanced risk management processes.

But using AI does not guarantee positive outcomes. Risk teams need to be vigilant to protect against error amplification and the integration of new systemic risks into firms.

For example, many firms are encouraging employees to use AI to help produce work output such as emails, reports and presentations. However, early-stage academic studies have reported that using AI in this way can create a mental distance between the individual and "their" output, and can negatively impact cognitive ability, "ownership" and quality of the reports and conclusions they produce. This doesn't mean that AI implementation should stop, but risk, compliance and technology teams must recognize the nuances in the balance between benefit and risk and work to solve the problems as they surface.

Although the legal and regulatory environment is still developing, there are already clear compliance regimes that need to be integrated into AI development and deployment. Aside from the EU AI Act and other emerging laws and standards, compliance teams in Financial Services are able to point to existing regulatory frameworks to drive risk and compliance activity. This article explores two relevant legal and regulatory levers that Risk and Compliance teams can use to drive ethical innovation with AI: the existing Financial Conduct Authority (FCA) principles and the EU Digital Operational Resilience Act (DORA). The FCA are encouraging their firms to innovate with AI, so act now to embed their core principles in your AI deployment.

Three FCA principles to prioritize in your AI Risk Compliance regime

Three of the 12 FCA principles are particularly important to your AI Risk Compliance regime. The table below sets-out these three principles, summarizes their relevance to AI risk and explains why they deserve particular focus to help ensure that AI technologies are deployed responsibly and ethically within your organization.

FCA principle	Relevance to AI risks	Systemic impact
Integrity (Principle 1): A firm must conduct its business with integrity.	AI systems can inadvertently lead to unethical outcomes, such as biased decision-making or manipulation of customer data. Upholding integrity ensures that firms are committed to ethical practices in their AI deployments, which is essential for maintaining trust with customers and regulators.	A firm's reputation can be significantly impacted by how it uses AI. By prioritizing integrity, firms can avoid practices that may be perceived as deceptive or harmful, thereby protecting their brand and fostering long-term relationships with clients.
Management and Control (Principle 3): A firm must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems.	The complexity and rapid evolution of AI technologies necessitate strong governance and risk management frameworks. This principle emphasizes the importance of having adequate controls in place to manage the specific risks associated with AI, such as operational failures, data privacy issues, long-term de-education of the workforce and erosion of decision ownership.	By focusing on management and control, firms can proactively identify and address potential risks before they escalate into significant issues. This is particularly important in the context of AI, where the consequences of failures can be substantial and far-reaching.
Customers' Interests (Principle 6) A firm must pay due regard to the interests of its customers and treat them fairly.	AI technologies could make decisions that directly affect customers, such as credit scoring, loan approvals, and personalized financial advice. Ensuring that AI systems prioritize customer interests is vital for delivering fair and beneficial outcomes.	By aligning AI practices with this principle, firms can demonstrate their commitment to treating customers fairly and complying with FCA expectations. Auditability is crucial for avoiding penalties and maintaining market access.

Following these principles leads to several practical steps firms can take now, to ensure they are robustly managing the risks associated with AI.

Define, control, manage: 3 practical steps firms can take now to promote innovation with AI

To apply these principles, you'll need to review existing operational controls to ensure they are updated to respond to the latest risks and opportunities presented by AI. AI is developing quickly, so the three steps below will need to be reviewed more regularly than for other principal risks.

1 Define and understand AI risk:

You should develop a clear and concise definition of "AI risk" that encompasses the potential forms of loss and the factors that could lead to those losses. To operationalize your definition, identify specific activities within your organization that could drive AI risk. Understanding the nuances of AI risk, and setting it out as a principal risk, will enable you to better manage and mitigate these risks effectively.

2 Establish a robust AI risk control framework:

You should create a comprehensive Risk Control Framework (RCF) tailored to AI, incorporating specific control domains and operational policies. This framework should ideally reflect international standards and laws – NIST AI 600, ISO42001 and EU AI Act as a minimum. And it should include clearly defined control domains and sub-domains that address the specific aspects of AI risk management. Engage with relevant operational teams, such as legal, data, technology and privacy experts, to embed required control enhancements into their day-to-day operational processes.

3 Implement continuous AI risk assessments:

To ensure that AI is being used in accordance with FCA principles, you should conduct regular AI risk assessments. These assessments should be dynamic, practical and align with responsible AI principles as well as current and emerging legal requirements. By continuously tracking regulatory developments and adapting assessment processes, firms can maintain a proactive stance in managing AI-related risks.

Operational resilience regimes will be an important lever to manage the systemic risks posed by AI

The Digital Operational Resilience Act (DORA) is a great example of a modern operational resilience regime. It aims to enhance the resilience of financial institutions in the European Union against various operational risks related to information and communication technology (ICT). DORA's objectives collectively aim to create a more resilient financial ecosystem capable of withstanding and recovering from operational disruptions, particularly those arising from technological vulnerabilities. AI is not specifically called out in DORA, but it is a technology whose deployment could introduce a systemic vulnerability to your operations. To future-proof your operational resilience and regulatory compliance, align AI governance and RCF development with your DORA implementation. DORA's objectives – set-out below align perfectly with the three practical steps you read in the previous section.

Strengthen ICT risk management:	DORA seeks to establish a comprehensive framework for managing ICT risks across financial institutions, ensuring that they have robust systems and processes in place to identify, assess, and mitigate potential threats. Embed AI risk controls within your IT governance and operations.
Enhancing incident reporting:	The act mandates timely and effective reporting of ICT-related incidents to relevant authorities, promoting transparency and enabling better coordination during crises to minimize the impact on financial stability. Include AI reporting in an upgraded incident reporting operating model that is tuned to the nuances of AI incident identification.
Promoting third-party risk management:	DORA emphasizes the importance of managing risks associated with third-party service providers, requiring financial institutions to conduct thorough due diligence and maintain oversight of their ICT service providers. Embed AI-related contract and risk due diligence in third-party risk programs.
Establishing testing and resilience requirements:	The regulation introduces requirements for regular testing of ICT systems and processes to ensure operational resilience, including stress testing and scenario analysis to evaluate the effectiveness of contingency plans. Review and align to the conformity assessment regime required by AI regulations.
Fostering a culture of operational resilience:	DORA aims to cultivate a culture of operational resilience within financial institutions, encouraging them to prioritize resilience in their strategic planning and decision-making processes. Review and uplift the AI RCF and Governance regime.

Contact

Matt Whalley

EY Digital Trust Platform Global Solution Lead
Ernst & Young LLP
Email: mwhalley1@uk.ey.com | Phone: +44 73 4202 1429

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 008634-25Gbl
BMC Agency GA 14285028
ED None