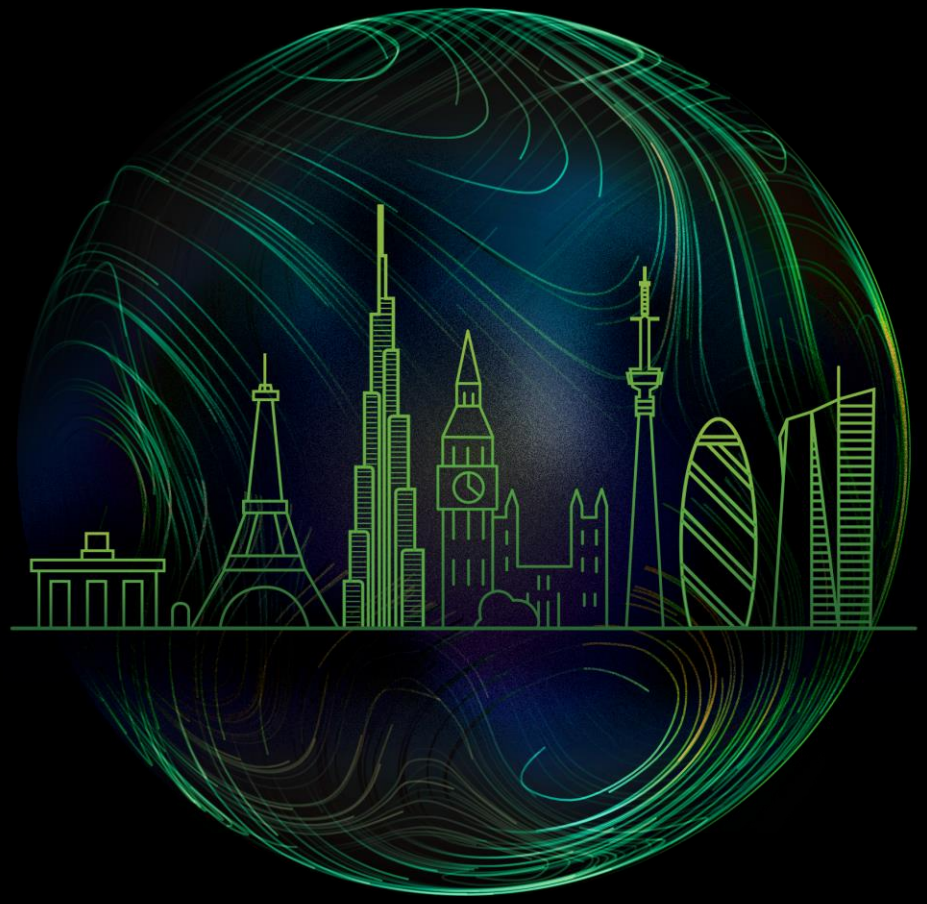
Deloitte.



Innovation, Payments and Digital Assets

Financial Markets Regulatory Outlook 2024

CENTRE *for*
REGULATORY
STRATEGY
EMEA

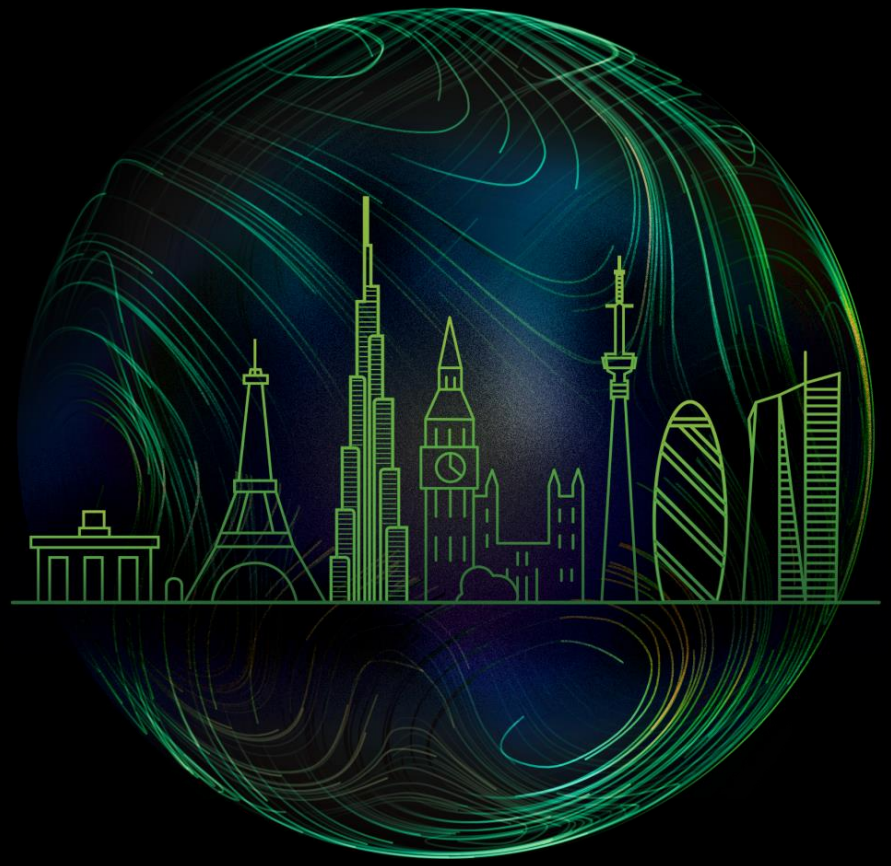
Regulatory Outlook 2024

Innovation, payments and digital assets – at a glance

Retail payments regulations
A strategic approach is key to responding to a new wave of regulatory change - 3

Digital assets
Navigating an evolving and fragmented landscape - 4

Artificial Intelligence and data
Implementation of new AI and Digital ID frameworks gets underway - 5



Retail payments regulations

A strategic approach is key to responding to a new wave of regulatory change

Impact Areas

Governance | Strategy | Finance | Operations | Control functions (Risk/Compliance/IA)

KEY CHALLENGES

- Regulation, combined with market forces, will continue to drive the separation of customer relationships and payment initiation from account provision and processing infrastructure. They will also enable the expansion of payment types (e.g., instant payments and stablecoins) and channels (e.g., embedded and mobile payments).
- To remain competitive and profitable, firms must re-evaluate their position in the value chain, offerings, pricing, technology stack, and strategic partnerships. However, mandatory regulatory spending will challenge their financial and operational capacity to invest in new business and technological capabilities.

WHAT'S HAPPENING THIS YEAR?

- The EU's review of payment and e-money regulations will intensify. Although final PSD3/PSR rules are unlikely before 2025, the proposals' key strategic elements are already clear. Non-bank PSPs will face tougher prudential rules and re-authorisation requirements, but also fairer access to payment systems. Banks will need to invest in dedicated TPPs' open banking API interfaces. Enhanced consumer protection and fraud refund rules – akin to those introduced by the UK's PSR – are likely to pose compliance and financial challenges for many PSPs.
- The EU IPR will become law in H1, requiring PSPs to offer instant euro payments at no additional cost and implement IBAN verification services and stricter sanctions screening. Compliance challenges will vary by Member States' instant payment adoption. But combined with open banking and Digital ID wallets, the IPR offers a strategic opportunity to develop cost-effective digital payment solutions, including alternatives to cards.
- The UK is also reviewing its payment framework. The FCA will bolster both the safeguarding and prudential regimes for payments, while also reviewing EU-derived payment authentication and contactless limit rules. HMT also committed to legislate to support wider adoption of open banking-enabled payments. The goal is a post-Brexit framework that improves resilience, fraud prevention, and customer experience.
- Concerning stablecoins, EU MiCAR requirements for issuers will be effective from June, whilst the UK will propose final rules by year-end with implementation by 2025. Regulatory clarity will help firms assess retail use cases, e.g. cross-border payments. Investment decisions will be influenced by other developing policies – e.g. final go/no-go for EU/UK CBDCs, growth of open banking payments, and infrastructure upgrades (e.g. UK NPA).

KEY ACTIONS FOR PAYMENT FIRMS IN 2024

Strategy

- Evaluate the aggregate impact of regulatory changes on products, channels, pricing, and strategic partnerships and acquisitions - including outside FS. Consider both payment and cross-sector rules, such as operational resilience.
- Identify regulatory developments that may influence the timing or outcome of strategic decisions, e.g., CBDC decisions or measures to promote A2A payments.
- Identify synergies between regulatory compliance and business innovation. E.g., leveraging Digital ID or open banking to build user-friendly omnichannel capabilities, brand trust and loyalty, payment security, and consumer protection.

Operations and finance

- Assess and improve IT architecture and business processes to ensure they can handle high-volume instant payment processing, including liquidity management, payee verification, fraud detection, reporting, and customer support.
- Enhance anti-fraud capabilities by investing in data, AI, and advanced biometrics to improve fraud detection, safeguard customers from harm across channels, and minimise the impact of reimbursement costs related to APP and other scams.

Control functions

- Enhance risk and compliance functions' capacity, expertise and technological capabilities to ensure they can respond both to new and increasing regulatory requirements and the fast pace of technological and business innovation.
- As use of data, AI and biometrics increase for both business and compliance purposes, review systems and controls for data governance and RMFs and ensure they align with emerging regulations.

Digital assets

Navigating an evolving and fragmented landscape

Impact Areas

- Governance
- Strategy
- Finance
- Operations
- Control functions (Risk/Compliance/IA)

KEY CHALLENGES

- Tokenisation will dominate regulated FS firms' digital asset pilots, with a particular focus on the issuance of tokenised bonds. Participation in EU/UK regulatory sandboxes will be helpful for "first mover" trading and settlement venues to emerge and pave the way for secondary markets.
- Intermediaries in unbacked digital asset markets, such as custodians and exchanges, who choose to be regulated under MiCAR, must finalise their EU location strategy. They must also build risk, compliance, and regulatory engagement capabilities to support successful authorisations.

WHAT'S HAPPENING THIS YEAR?

- Two regulatory developments may facilitate FS firms' tokenisation pilots – the issuance of a digital representation of an asset on DLT. A new UK sandbox will enable firms to set-up and test DLT-based FMI, complementing the EU version launched in 2023. Meanwhile regulated stablecoins under new EU/UK regimes may enable faster settlement of tokenised securities.
- Building initial capabilities in the sandboxes will be a helpful investment for firms with ambitions to establish market leading trading and settlement venues. These includes FMIs, leveraging existing licences and capabilities, and new players. Sandbox firms can seek certain exemptions from securities rules (e.g. MiFID/MiFIR and CSDR) necessary to trade and settle tokenised securities. To maximise chances for selection, firms need to demonstrate a viable growth plan and the ability to scale risk management capabilities as pilots mature.
- Global firms must navigate a fragmented[1] regulatory landscape for unbacked digital assets (e.g. Bitcoin). In the EU, a patchwork of MiCAR and local regimes will apply between 2024 and 2026. Varying local regulations and regulator capabilities may require firms to adopt a short- and medium-term location and offering strategy. Implementing MiCAR will be complicated by the need for agile compliance strategies as technical standards are finalised and the concurrent implementation of broader FS rules (e.g. DORA).
- The UK framework for unbacked digital assets is less developed. Detailed rules will start to emerge this year but are unlikely to be finalised until end-2024. Compliance deadlines will not kick in before well into 2025. But firms should shape their UK strategy and cross-border capabilities and offerings in response to any consultations.

KEY ACTIONS FOR FIRMS IN 2024

Strategy

- Consider role in future DLT-based value chain and business case for participation in sandboxes, assessing cost of getting additional regulatory licences, if required.
- Maintain view of partners and competitors as tokenisation pilots progress.
- Finalise EU location strategy. Key factors to consider include local approaches to MiCAR implementation, access to talent, bank accounts and payment infrastructure.
- Evaluate impact of MiCAR on service offering expansion plans.

Finance and operations

- Refine tokenisation operating model based on sandbox lessons learned and regulatory feedback.
- Enhance and demonstrate skills and capabilities to maintain financial and operational resilience in MiCAR authorisations. E.g. include realistic financial forecasts and develop and test a business continuity plan.

Control functions

- Embed risk and compliance in tokenisation pilots, building knowledge of new/enhanced DLT risks. May reduce time-to-market if pilots mature.
- Demonstrate the robustness and effectiveness of client asset segregation and conflict-of-interest management arrangements in MiCAR authorisations.
- Consider deploying policies and procedures developed to MiCAR standards in UK arm if part of a group. This will serve as a baseline for compliance which firms can tailor later. Reputational risk management benefits may outweigh compliance costs.

Artificial Intelligence and data

Implementation of new AI and Digital ID frameworks gets underway

Impact Areas

Governance | Strategy | Finance | Operations | Control functions (Risk/Compliance/IA)

KEY CHALLENGES

- The EU AIA, the first comprehensive AI-specific legislative framework, will become law. Compliance requirements for high-risk use cases will affect the cost-benefit analysis for current or future use. Strict requirements for AI developers will increase the strategic importance of buy or build decisions.
- Global firms must choose between developing EU-specific AI offerings or applying EU standards universally. UK firms may choose to adopt specific AIA elements, where detailed guidance on implementing the UK outcome-focused framework is needed.

WHAT'S HAPPENING THIS YEAR?

- The EU AIA will take effect in H1, beginning a phased two-year implementation. It imposes strict requirements on the use of high-risk systems and General Purpose AI models. However, AIA technical standards will not emerge until later in 2024/25, making impact assessments and compliance strategies more complex. AI developers face more substantial obligations than firms that solely deploy AI, including pre-market conformity assessments. Defining firms' role(s) for each AI use case and navigating grey areas will be a top priority.
- AIA rules will intersect with other existing EU regulatory frameworks, such as GDPR and DORA. Identifying and addressing the tensions and synergies between cross-sectoral and FS rules and the AIA will require careful consideration, and the overlaps will vary depending on the specific use cases at hand.
- The UK Government is expected to confirm its proposed non-statutory principle-based AI regulatory approach, which will rely heavily on existing technology-neutral rules. To scrutinise AI risks, the FCA, BoE, and ICO will leverage key frameworks such as the Consumer Duty, MRM, operational resilience, and UK GDPR. Firms must ensure full compliance with these rules through their AI governance and RMFs. Regulators will publish more guidance to help firms interpret existing requirements in an AI context, but details/timings are not yet known.
- The EU and UK are also both promoting Digital IDs to simplify and secure identification and data sharing, albeit with different approaches. The EU will mandate FS firms to accept EUDIW for strong user authentication. The UK is set to establish a Digital ID trust framework by end-2024, which will grant Digital IDs the same legal status as paper documents, although acceptance will remain voluntary.

KEY ACTIONS FOR ALL REGULATED FINANCIAL SERVICES FIRMS IN 2024

Governance and strategy

- Understand exposure to new and existing AI-relevant requirements by creating an inventory of current and planned AI use cases, focusing on high-risk ones.
- Determine role in value chain for each use case (developer vs deployer). Investigate grey areas resulting from significant customisation of third-party AI systems.
- Create a strategic response plan and clear accountability lines for AI use cases affected by the new AIA requirements. If operating globally, decide whether to develop EU-specific solutions or apply EU AI governance standards globally.
- Assess which Digital ID use cases can provide strategic advantages, such as improved customer experience, efficiency, and new services/products. Consider competition from both FS and non-FS firms for customer relationships and trust.

Operations

- Ensure that AI systems, IT architecture, and operations comply with regulatory requirements for AI. Focus on data governance, MRM, human oversight, transparency, operational resilience, monitoring, and reporting.
- Ensure IT systems and business processes (e.g., KYC/AML, SCA, and CRM) can support voluntary (UK) and mandated (EU) Digital ID frameworks/wallets.

Control functions

- Enhance RMFs, policies and procedures to align with AI-specific and technology-neutral rules. Address potential tensions and interaction between requirements. E.g., AI-specific rules vs data and consumer protection or outsourcing rules.
- In the absence of granular regulatory guidance, UK firms can look to the EU AIA – e.g., concerning data quality and or accuracy – as a benchmark for AI RMFs, albeit allowing for tailoring as appropriate.

Glossary

A2A
Account-to-Account

AI
Artificial Intelligence

AIA
Artificial intelligence Act

AML
Anti Money-Laundering

API
Application Programming Interface

APP
Authorised Push Payment

BoE
Bank of England

CBDC
Central Bank Digital Currency

CRM
Customer Relationship Management

CSDR
Central Securities Depositories Regulation

DLT
Distributed Ledger Technology

DORA
Digital Operational Resilience Act

EUDIW
EU Digital Identity Wallets

FCA
Financial Conduct Authority

FMI
Financial Market Infrastructure

FS
Financial Services

GDPR
General Data Protection Regulation

HMT
His Majesty's Treasury

IA
Internal Audit

IBAN
International Bank Account Number

ICO
Information Commissioner's Office

IPR
Instant Payments Regulation

IT
Information Technology

KYC
Know Your Client

MICAR
Markets in Crypto-Assets Regulation

MiFID
Markets in Financial Instruments Directive

MiFIR
Markets in Financial Instruments Regulation

MRM
Model Risk Management

NPA
New Payments Architecture

PSD3/PSR
Third Payment Services Directive / Payment Services Regulation

PSP
Payment Service Provider

PSR
Payment Systems Regulator

RMF
Risk Management Framework

SCA
Strong Customer Authentication

TPP
Third-Party Provider

CENTRE *for*
REGULATORY STRATEGY
EMEA

The Deloitte Centre for Regulatory Strategy is a powerful resource of information and insight, designed to assist financial institutions manage the complexity and convergence of rapidly increasing new regulation.

With regional hubs in the Americas, Asia Pacific and EMEA, the Centre combines the strength of Deloitte's regional and international network of experienced risk, regulatory, and industry professionals – including a deep roster of former regulators, industry specialists, and business advisers – with a rich understanding of the impact of regulations on business models and strategy.

Download this report, and more like it, at Deloitte.co.uk/ECRS

Deloitte.

Designed by CoRe Creative Services. RITM1530152