



INVENIRE RISK

WHITE PAPER / Q2 2026

RegTech at an inflection point

Emerging technologies, regulatory transformation and the future of financial crime compliance

A board and executive assessment across the US, UK, EU
and major Asian financial centres

FINANCIAL CRIME / AI & DATA / SUPTECH

QUANTUM / DIGITAL IDENTITY / REGULATORY CHANGE

Risk expertise. Connected.

Inside this paper

An evidence-led assessment of how emerging technology, supervisory innovation and regulatory change are reshaping financial-crime compliance and risk management.

Executive summary and the changing purpose of RegTech.....3

Financial crime: from isolated alerts to connected intelligence.....4

Regulatory divergence and supervisory convergence.....5

SupTech: when supervisors become data-driven.....6

Privacy, identity and interoperability.....7

Quantum computing and the financial-crime frontier.....8

The risk introduced by RegTech.....9

The outlook to 2030 and conclusion.....10

References.....11

THREE CONNECTED THEMES

01	Regulation & SupTech	How regulatory regimes differ - and how data-driven supervision may increase expectations for evidence, consistency and auditability.
02	Financial crime & technology	How ML, graph analytics, generative AI, privacy technologies and digital identity can strengthen detection and investigation.
03	The technology frontier	How quantum computing, AI-native operating models and new technology risks could reshape compliance through 2030.

About this edition

This Q2 2026 white paper applies an evidence cut-off of 30 June 2026. It is designed for board directors, Chief Risk, Compliance and Technology Officers, and senior leaders in banking and capital markets. General information and risk commentary, not legal advice. Jurisdiction-specific applicability requires independent assessment. The analysis distinguishes requirements already in force at the cut-off date from later effective dates and forward-looking scenarios. Primary regulatory, supervisory and technical sources are prioritised throughout, supplemented by peer-reviewed research where appropriate.

Executive summary

Regulatory technology is shifting from discrete compliance utilities toward a connected layer of data, decision support and supervisory evidence. The change is especially consequential for banks and capital-markets firms because financial-crime controls increasingly operate across customer identity, transaction monitoring, sanctions, case management, reporting and model governance. The Financial Stability Board has linked RegTech and SupTech growth to greater data availability, cloud infrastructure and APIs, while FATF has encouraged responsible adoption of technology to improve AML/CFT effectiveness. [1,2]

This paper argues that the next competitive distinction is not simply the sophistication of an algorithm. It is whether institutions can connect customer identity, ownership, payments, network behaviour, investigative decisions and regulatory evidence without losing provenance or accountability. BIS Innovation Hub work on collaborative analytics and payment-system analysis illustrates the potential value of network-level views, while also highlighting data, privacy, legal and operational constraints. [4,5]

The 2026-2030 outlook is therefore one of selective convergence, not frictionless automation. Machine learning and graph analytics can strengthen detection; generative AI can help investigators navigate evidence; privacy-enhancing technologies can support controlled collaboration; and supervisors are themselves becoming more data-driven. At the same time, model risk, explainability, third-party concentration, cyber risk, data quality and governance remain material constraints. Quantum computing adds a longer-horizon discontinuity for cryptography, but not a demonstrated near-term transformation of AML analytics. [3,7,17,28-32]

The changing purpose of RegTech

Early RegTech investment frequently targeted the cost of compliance: screening, monitoring, reporting, workflow and document capture. Its emerging purpose is broader: to improve the quality, consistency and timeliness of risk decisions and the evidence that supports them. This is consistent with the FSB view that RegTech and SupTech can improve surveillance, regulatory reporting and analytical capability, and with FATF work on technology-enabled AML/CFT. [1,2]

The strongest architecture connects five layers: trusted identity and beneficial-ownership data; transaction and counterparty information; detection models and scenario rules; human investigation and decision records; and supervisory or regulatory reporting. BIS Project Aurora and Project Hertha demonstrate why connecting data and network context can expose patterns that institution-by-institution monitoring may miss, while also reinforcing the need for privacy, explainability and robust feedback loops. [4,5]

A market of unequal maturity

Traditional screening and rules engines are mature, as are many case-management products. Supervised machine learning, entity resolution and graph analysis are established capabilities but their performance varies with data quality and labelling. Generative AI is moving quickly into analyst-assistive use cases, yet prudential authorities continue to treat model governance, validation and accountability as central concerns. In April 2026, US agencies revised their model-risk guidance while explicitly stating that generative and agentic AI were novel and outside the scope of that guidance; the UK PRA continued to apply model-risk principles, including to AI and machine-learning techniques where they fall within model use. [3,7,17,18]

From isolated alerts to connected intelligence

AML programmes confront layering, mule networks, trade-based laundering, sanctions evasion, synthetic identities and cross-border opacity. Individual transaction rules can identify thresholds and simple typologies; sophisticated criminal networks often require an entity- and network-level view. FATF has highlighted the potential of advanced analytics and collaborative approaches, while BIS experiments have tested graph and AI techniques across synthetic multi-institution and payment-system data. [2,4,5,25]

Machine-learning approaches can help rank alerts, detect anomalous sequences and identify combinations of signals that fixed rules do not capture. Their governance challenge is unusually acute: confirmed criminal activity is sparse, labels can be delayed or biased, and historical investigator decisions can encode earlier control assumptions. Effective use therefore requires risk-based monitoring, validation, outcome analysis and governance rather than reliance on model performance metrics alone. [2,6,7,17]

Generative AI and agentic workflows

Generative AI can assist with adverse-media synthesis, extracting facts from corporate documents, translating multilingual evidence and preparing investigation narratives. A more ambitious agentic system could gather approved evidence, query sanctioned data sources and prepare a case for human review. The control challenge grows with autonomy: hallucination, prompt manipulation, unauthorised tool use, incomplete provenance and over-reliance can turn an efficiency tool into a source of compliance risk. The FSB identifies model risk, data quality, cyber risk and third-party dependency among material AI-related vulnerabilities; US and UK supervisory material likewise emphasises governance and validation. [3,7,17,18]

For sanctions screening, false-positive reduction is valuable only if recall of true matches is maintained across names, scripts and jurisdictions. Institutions should distinguish performance on curated test datasets from performance in live operational conditions, document thresholds and escalation logic, and retain evidence for material overrides. OFAC frames an effective sanctions compliance programme around management commitment, risk assessment, internal controls, testing/auditing and training; the FCA Financial Crime Guide similarly emphasises effective systems and controls, including sanctions and transaction monitoring. [8,16]

Regulatory divergence and supervisory convergence

United States

The United States combines the Bank Secrecy Act/AML framework, FinCEN administration, OFAC sanctions requirements and sector-specific prudential and securities supervision. The direction of travel is not uniformly toward more prescriptive technology rules. FinCEN's March 2025 interim final rule narrowed Corporate Transparency Act beneficial-ownership reporting to certain foreign entities registered to do business in the United States, materially changing the available reporting landscape. In April 2026, the OCC, Federal Reserve and FDIC revised model-risk guidance, rescinded the prior BSA/AML model-risk statement and explicitly placed generative and agentic AI outside the scope of the revised guidance pending further work. For institutions, the result is a technology environment governed by underlying BSA/AML, sanctions, safety-and-soundness and control expectations rather than a single RegTech rulebook. [6-9]

European Union

The EU is moving toward a more harmonised AML framework and a central AML authority, alongside GDPR, digital-identity developments, DORA and the AI Act. Regulation (EU) 2024/1624 creates a directly applicable AML rulebook scheduled, in general, to apply from 10 July 2027, while Regulation (EU) 2024/1620 establishes AMLA. DORA has applied since 17 January 2025. At the 30 June 2026 evidence cut-off used for this paper, the original AI Act timetable provided for general application from 2 August 2026, with specified provisions already applying earlier; later amendments are outside this edition. The European Digital Identity Framework also expands the policy infrastructure around trusted digital identity. For RegTech providers and users, the strategic implication is that AML, AI, privacy, operational resilience and identity obligations increasingly intersect rather than operate as separate compliance domains. [10-15]

United Kingdom

The UK retains a distinctive financial-crime and sanctions regime, with the FCA, PRA, HM Treasury and relevant enforcement bodies occupying different roles. The FCA updated its Financial Crime Guide in November 2024, including material on sanctions, proliferation financing and transaction monitoring. For banks, the PRA's current SS1/23, published in April 2026, sets five principles for model risk management and expressly includes the management of AI and machine-learning risks where relevant to model use. Earlier joint Bank of England/PRA/FCA work on AI and machine learning also highlighted third-party, model and data-governance issues. The practical message is that technology-enabled compliance remains anchored in demonstrable systems and controls, senior accountability and proportionate model governance. [16-18]

Singapore, Hong Kong and wider Asian hubs

Singapore and Hong Kong have developed active RegTech and supervisory-technology ecosystems, while Japan has increasingly formalised its dialogue on responsible AI in finance. MAS has maintained FEAT principles for responsible AI and data analytics and operates COSMIC, a platform that enables participating financial institutions to share information on customers exhibiting specified financial-crime red flags. HKMA has published AML/CFT RegTech case studies and a RegTech Adoption Practice Guide. Japan's Financial Services Agency published version 1.1 of its AI Discussion Paper in March 2026 and has also updated AML/CFT guidance and FAQs. These approaches illustrate a practical Asian policy theme: encourage innovation and information use while retaining clear governance, privacy and supervisory accountability. [19-24]

When supervisors become data-driven

SupTech changes the relationship between firms and authorities. Supervisors can use text analytics to review filings, anomaly detection to prioritise entities and network analysis to connect patterns across institutions. The FSB has described SupTech as a means of improving oversight, surveillance and analytical capability, while later work has encouraged authorities to strengthen their own AI-enabled supervisory capacity. [1,3]

For boards, this has two implications. First, inconsistent regulatory data and weak audit trails may become more visible as supervisory analysis improves. Second, firms should not assume that supervisors will accept an automated output simply because it is generated by sophisticated technology. The evidential chain - source data, transformation, model or rule, decision, review and override - remains central. [1,3,27]

What changes when the regulator can analyse at scale?

The practical consequence may be a shift from periodic, sample-based scrutiny toward more data-intensive supervision. That does not eliminate supervisory judgment; it changes the amount and granularity of evidence available to support it. BIS/FSI research on SupTech stresses that moving from experimentation into supervision requires integration with supervisory processes, data quality, governance, skills and sustainable operating models. [27]

The strategic issue is not simply whether a regulator adopts AI. It is whether firms can produce machine-readable, internally consistent regulatory evidence while retaining human accountability and legal defensibility. That increases the importance of common identifiers, controlled taxonomies, data lineage and reproducible decision records. [1,3,27]

Privacy, identity and interoperability

Financial crime is frequently cross-institutional, while the data needed to expose it is fragmented. Privacy-enhancing technologies - including secure multiparty computation, homomorphic encryption, private set intersection and related cryptographic techniques - can in some circumstances permit joint analysis without broadly exposing underlying sensitive data. FATF's stocktake treats these technologies as promising but stresses that their deployment must remain consistent with applicable data-protection and privacy frameworks, data quality and legal authority for sharing. [25]

Digital identity can improve onboarding, authentication and evidence reuse, but it cannot by itself establish that a customer is low risk or that a beneficial-ownership record is accurate. FATF's digital-identity guidance therefore treats suitability and reliability as part of a risk-based CDD assessment. Similarly, blockchain traceability can improve visibility into some virtual-asset flows without eliminating off-chain identity gaps, cross-chain complexity or the need for investigation. [26,33]

Interoperability is becoming a control issue

As RegTech becomes more modular, institutions increasingly depend on data and decision flows across identity providers, screening engines, case-management tools, cloud platforms and internal data estates. Interoperability is therefore a control issue as well as an architecture issue: schema changes, stale data, API failure or inconsistent identifiers can alter the effectiveness of a compliance process. The FSB's RegTech/SupTech work identifies APIs and cloud infrastructure as important enablers, while DORA makes ICT and third-party resilience a central financial-sector concern in the EU. [1,12]

For senior leaders, this shifts attention from selecting individual tools toward governing the interfaces between them. A technically strong AML model is of limited value if identity data arrive late, sanctions lists are stale, ownership links are lost between systems or investigators cannot reconstruct the basis of an alert. Data standards, lineage, reconciliation and exception handling are therefore part of the financial-crime control environment. [2,16,25]

Quantum computing and the financial-crime frontier

A credible threat, but an uncertain timetable

Quantum computing is not one capability with one arrival date. Noisy experimental systems, error-corrected prototypes and cryptographically relevant fault-tolerant machines have very different implications. Current public guidance does not establish that a machine capable of breaking production-scale public-key cryptography will arrive within five years. However, the Federal Reserve Bank of Philadelphia has highlighted expert survey expectations spanning roughly five to fifteen years, while NIST and the UK NCSC are already directing organisations toward post-quantum migration. The NCSC recommends discovery and initial planning by 2028, highest-priority migrations by 2031 and broad completion by 2035. [28-31]

How quantum capability could change criminal opportunity

At sufficient fault-tolerant scale, quantum computation would alter the security assumptions underpinning much of today's asymmetric cryptography. Shor's algorithm is particularly relevant because it provides a quantum method for solving the mathematical problems on which RSA and widely deployed elliptic-curve cryptographic schemes depend. The resulting exposure would extend beyond encrypted communications to digital signatures, authentication, identity infrastructure and other systems whose trust models rely on these cryptographic primitives. This is not a claim that current quantum hardware can defeat modern banking cryptography at scale. The nearer-term risk is the long migration lead time, including the possibility that encrypted information captured today could be retained for later attack. NIST finalised its first three post-quantum cryptography standards in August 2024 and has separately published transition guidance. [28-31]

It is plausible that concentrated access - including access by well-funded state organisations - could create asymmetric capability before fault-tolerant quantum computing becomes broadly commercial. That is a scenario, not an observed fact about current operational access. For financial institutions, the governance response is therefore to treat quantum as a cryptographic-agility and information-longevity issue: identify vulnerable algorithms and dependencies, classify data by confidentiality lifetime, understand supplier roadmaps and avoid tying critical infrastructure to cryptography that cannot be replaced. [29-31]

Could quantum help AML defenders?

Researchers are exploring quantum optimisation, search, kernel methods and quantum-enhanced machine learning for pattern recognition and network problems. In principle, certain mathematical subroutines may offer speedups relevant to optimisation or analytics. In practice, evidence of useful quantum advantage for real-world AML workloads remains limited, and the academic literature emphasises unresolved challenges in trainability, data encoding, noise, benchmarking and identifying tasks where quantum approaches outperform strong classical methods. [32,33]

Large-scale AML organisations could ultimately benefit from hybrid workflows in which classical systems prepare features, quantum resources solve a tightly defined optimisation or sampling task and conventional analytics validate results. That possibility should be treated as research and experimentation rather than a near-term operating-model assumption. For the 2026-2030 horizon, post-quantum cryptographic migration is substantially more actionable than a wholesale redesign of transaction monitoring around quantum computing. [28-33]

The risk introduced by RegTech itself

Technology can reduce one category of compliance risk while increasing another. Model drift can degrade detection; poor data quality can create confident but incorrect outputs; opaque vendors can impede assurance; cloud and model concentration can create systemic dependencies; and automation can accelerate errors. These concerns recur across FSB AI analysis, prudential model-risk guidance, DORA and UK supervisory expectations. [3,7,12,17]

The central trade-off: automation versus evidence

More automation can increase speed and consistency, but it also raises the cost of weak provenance. If a system cannot reconstruct which data, model, prompt, rule or external service contributed to a decision, the institution may struggle to investigate errors, justify outcomes or demonstrate control effectiveness. Model and AI governance therefore needs to preserve traceability across development, use, validation, monitoring and material overrides. [3,7,17]

This is particularly important for agentic systems that can call tools or trigger workflows. Access entitlements, permitted actions, source whitelists, approval gates and immutable event logs become part of the compliance control design. The April 2026 US interagency model-risk guidance explicitly describes generative and agentic AI as novel and rapidly evolving and leaves them outside its scope, underscoring that established model-governance frameworks do not automatically resolve all control questions raised by agentic systems. [7]

Third-party and concentration risk

RegTech stacks increasingly depend on cloud infrastructure, specialist data providers, model vendors and identity services. This creates a tension between modular innovation and dependency concentration. Institutions need exit options, service-level evidence, data-portability arrangements, resilience testing and a clear understanding of subcontractors and fourth parties. FSB AI analysis identifies third-party concentration as a potential financial-stability vulnerability, while DORA and UK supervisory material reinforce expectations around technology and model dependencies. [3,12,17]

The outlook to 2030

Three trajectories appear plausible. In a measured scenario, institutions incrementally combine rules, machine learning and analyst-assistive AI while regulators strengthen digital reporting. In a faster-convergence scenario, interoperable identity, collaborative analytics and AI-enabled supervision compress the distance between detection, investigation and supervisory insight. In a fragmented scenario, data restrictions, legacy estates, weak standards and inconsistent AI governance slow adoption and preserve parallel manual controls. These are Invenire scenarios rather than regulatory forecasts, informed by the adoption constraints identified in FSB and BIS/FSI work. [1,3,27]

The decisive strategic question for boards is not whether to acquire the newest RegTech capability. It is whether compliance, risk, technology and data leadership can create reliable information flows and accountable decision rights around it. The regulatory direction across major markets increasingly favours demonstrable governance, proportionality, resilience, validation and evidence over unqualified automation. [3,7,17,18]

Conclusion

By 2030, RegTech may be less recognisable as a standalone category and more embedded in the everyday infrastructure of risk management and supervision. The strongest use cases are likely to connect detection, investigation, identity, collaboration and reporting while preserving evidence and human accountability. FATF and BIS work suggests that collaborative analytics and network-level approaches can materially improve visibility into complex financial crime, but legal authority, privacy, data quality and operating-model design remain decisive constraints. [2,4,5,25,27]

Quantum computing introduces a potentially profound long-horizon discontinuity, but its immediate significance is preparedness rather than proven AML transformation. The organisations that progress most effectively will distinguish between what is deployable now, what deserves controlled experimentation and what requires strategic readiness. For quantum, that means beginning cryptographic discovery and migration planning while treating quantum-enhanced AML analytics as an emerging research field whose practical advantage remains unproven. [28-33]

References

- [1] Financial Stability Board (2020). The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market Developments and Financial Stability Implications. 9 October 2020. <https://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatory-technology-by-authorities-and-regulated-institutions-market-developments-and-financial-stability-implications/>
- [2] Financial Action Task Force (2021). Opportunities and Challenges of New Technologies for AML/CFT. 1 July 2021. <https://www.fatf-gafi.org/en/publications/Digitaltransformation/Digital-transformation.html>
- [3] Financial Stability Board (2024). The Financial Stability Implications of Artificial Intelligence. 14 November 2024. <https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/>
- [4] Bank for International Settlements, BIS Innovation Hub (2023). Project Aurora: The Power of Data, Technology and Collaboration to Combat Money Laundering across Institutions and Borders. Innovation Hub Project Report, 31 May 2023. <https://www.bis.org/publications/project-aurora-power-data-technology-and-collaboration-combat-money-laundering-across-institutions-and-borders>
- [5] Bank for International Settlements, BIS Innovation Hub (2025). Project Hertha: Identifying Financial Crime Patterns in Real-Time Retail Payment Systems. 5 June 2025. <https://www.bis.org/project/hertha>
- [6] Federal Financial Institutions Examination Council (2026). Bank Secrecy Act/Anti-Money Laundering Examination Manual. Online edition; February 2026 revisions. <https://bsaaml.ffiec.gov/manual>
- [7] Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System and Federal Deposit Insurance Corporation (2026). Model Risk Management: Revised Guidance. OCC Bulletin 2026-13, 17 April 2026. <https://occ.treas.gov/news-issuances/bulletins/2026/bulletin-2026-13.html>
- [8] US Department of the Treasury, Office of Foreign Assets Control (2019). A Framework for OFAC Compliance Commitments. 2 May 2019. https://ofac.treasury.gov/recent-actions/20190502_33
- [9] Financial Crimes Enforcement Network (2025). Beneficial Ownership Information Reporting Requirement Revision and Deadline: Interim Final Rule. 26 March 2025; see also FinCEN release of 21 March 2025. <https://www.fincen.gov/news/news-releases/fincen-removes-beneficial-ownership-reporting-requirements-us-companies-and-us>
- [10] European Parliament and Council (2024). Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. OJ L, 19 June 2024. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1624>
- [11] European Parliament and Council (2024). Regulation (EU) 2024/1620 of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism. OJ L, 19 June 2024. <https://eur-lex.europa.eu/eli/reg/2024/1620/oj>
- [12] European Parliament and Council (2022). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA). OJ L 333, 27 December 2022. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554>
- [13] European Parliament and Council (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). OJ L 119, 4 May 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [14] European Parliament and Council (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L, 12 July 2024. Citation reflects the law and timetable as at 30 June 2026. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- [15] European Parliament and Council (2024). Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. OJ L, 30 April 2024. <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- [16] Financial Conduct Authority (2024). PS24/17: Financial Crime Guide Updates. Policy Statement, 29 November 2024. <https://www.fca.org.uk/publications/policy-statements/ps24-17-financial-crime-guide-updates>
- [17] Prudential Regulation Authority (2026). SS1/23: Model Risk Management Principles for Banks. Current version published and effective 23 April 2026. <https://www.bankofengland.co.uk/prudential-regulation/publication/2023/may/model-risk-management-principles-for-banks-ss>
- [18] Bank of England, Prudential Regulation Authority and Financial Conduct Authority (2023). FS2/23: Artificial Intelligence and Machine Learning. Feedback Statement, 26 October 2023. <https://www.bankofengland.co.uk/prudential-regulation/publication/2023/october/artificial-intelligence-and-machine-learning>
- [19] Monetary Authority of Singapore (2018). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. 12 November 2018. <https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat>
- [20] Monetary Authority of Singapore (2024-2026). Anti-Money Laundering: COSMIC - Collaborative Sharing of ML/TF Information & Cases. MAS regulatory information page. <https://www.mas.gov.sg/regulation/anti-money-laundering>

- [21] Hong Kong Monetary Authority (2021). AML/CFT Regtech: Case Studies and Insights. 21 January 2021. <https://brdr.hkma.gov.hk/eng/doc-ldg/docId/20210121-1-EN>
- [22] Hong Kong Monetary Authority (2021). Regtech Adoption Practice Guide, Second Issue: AML/CFT. 26 July 2021. <https://brdr.hkma.gov.hk/eng/doc-ldg/docId/20210726-2-EN>
- [23] Financial Services Agency, Japan (2026). Preliminary Discussion Points for Promoting the Sound Utilization of AI in the Financial Sector: AI Discussion Paper, Version 1.1. 3 March 2026. <https://www.fsa.go.jp/en/news/2026/20260303/aidp.html>
- [24] Financial Services Agency, Japan (2024). Revision of Frequently Asked Questions Regarding Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism. 2 April 2024. <https://www.fsa.go.jp/en/news/2024/20240402/20240402.html>
- [25] Financial Action Task Force (2021). Stocktake on Data Pooling, Collaborative Analytics and Data Protection. FATF/OECD. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Stocktake-Datapooling-Collaborative-Analytics.pdf>
- [26] Financial Action Task Force (2020). Guidance on Digital Identity. FATF/OECD. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf>
- [27] Prenio, J. (2024). Peering through the Hype: Assessing SupTech Tools' Transition from Experimentation to Supervision. FSI Insights on Policy Implementation No. 58, Bank for International Settlements, 14 June 2024. <https://www.bis.org/fsi/publ/insights58.htm>
- [28] National Institute of Standards and Technology (2024). FIPS 203, FIPS 204 and FIPS 205: Post-Quantum Cryptography Standards. 13 August 2024. <https://www.nist.gov/news-events/news/2024/08/announcing-approval-three-federal-information-processing-standards-fips>
- [29] National Institute of Standards and Technology (2024). NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards. 12 November 2024. <https://csrc.nist.gov/pubs/ir/8547/ipd>
- [30] National Cyber Security Centre (2025). Timelines for Migration to Post-Quantum Cryptography. Guidance, 20 March 2025. <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>
- [31] Sanches, F. (2026). How Quantum Computing Threatens Cryptography. Economic Insights, Federal Reserve Bank of Philadelphia, 21 April 2026. <https://www.philadelphiafed.org/the-economy/banking-and-financial-markets/how-quantum-computing-threatens-cryptography>
- [32] Cerezo, M., Verdon, G., Huang, H.-Y., Cincio, L. and Coles, P.J. (2022). Challenges and Opportunities in Quantum Machine Learning. Nature Computational Science, 2, 567-576. doi:10.1038/s43588-022-00311-3. <https://doi.org/10.1038/s43588-022-00311-3>
- [33] Financial Action Task Force (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. 28 October 2021. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>

Research and citation note

This edition uses an evidence cut-off of 30 June 2026. References prioritise primary legislation, regulators, supervisors, international standard setters and central-bank or BIS research, supplemented by peer-reviewed academic literature for the quantum-computing discussion. Later developments are not used to restate the position as at the cut-off date. Forward-looking statements and scenarios are identified as analysis rather than enacted regulatory requirements.

INVENIRE RISK

Risk expertise. Connected.

invenirisk.com/contact | info@invenirisk.com

Q2 2026 edition. Evidence cut-off 30 June 2026. General information and risk commentary, not legal advice.