Deloitte.

Centre for
Regulatory Strategy
Asia Pacific

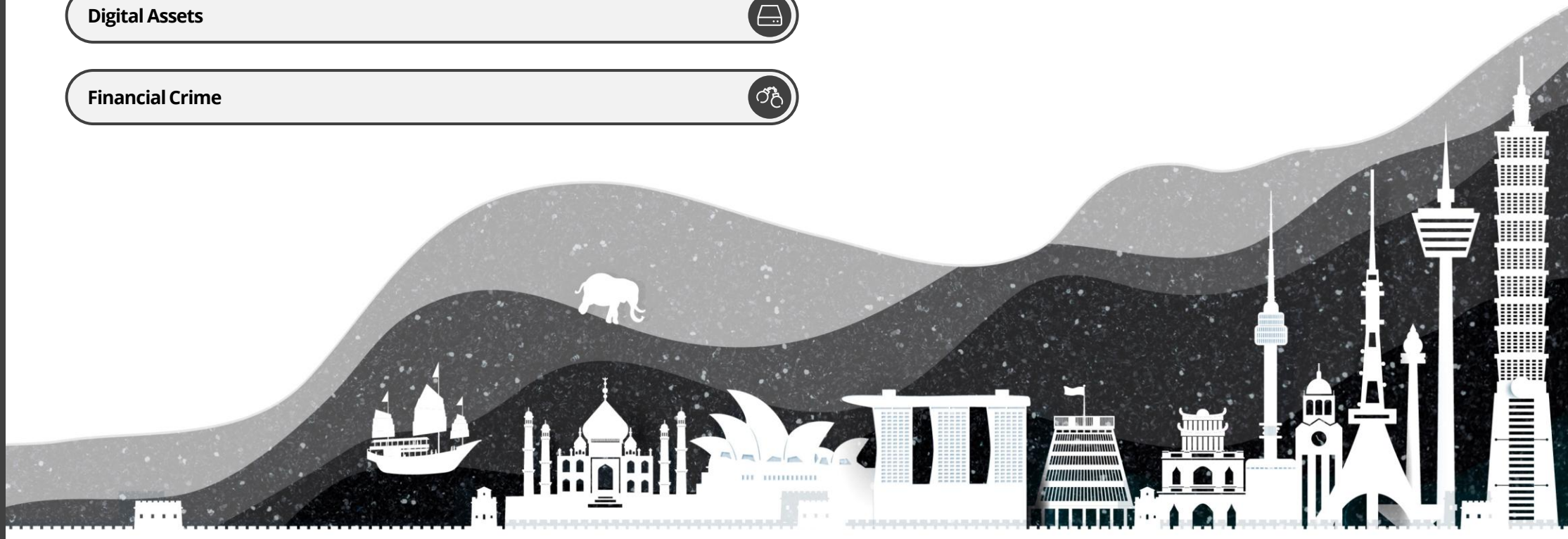
ACRS 2026 Financial Services Regulatory Outlook

Building Resilience in an Era of Disruption

February 2026

Navigating the Report

Click icon to navigate to the relevant section



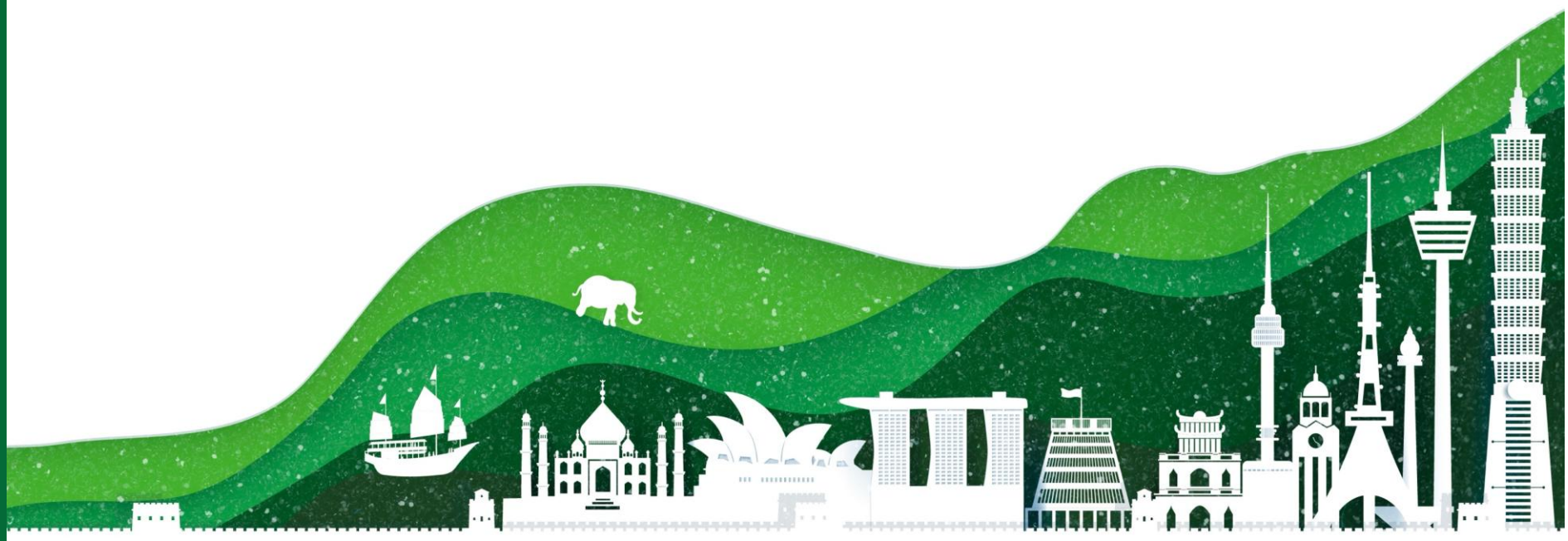
Global Foreword

As we enter 2026, governments and regulators worldwide are recalibrating financial regulation and supervision in pursuit of their own objectives.

This is no "big bang" liberalisation.[1] Policymakers are trying to reconcile three powerful, sometimes competing, forces: economic growth challenges, rapid innovation, and a difficult risk outlook. This outlook is increasingly characterised by hybrid risks that cut across financial, operational, technological and geopolitical domains.

Growth and productivity remain modest in many advanced economies, with inflation lower but still sticky in places. General-purpose technologies adopted by regulated institutions, chiefly Artificial Intelligence (AI) and blockchain, promise efficiency and growth but introduce new risks and vulnerabilities. A more volatile geopolitical and trading environment complicates cross-border finance and policymaking. The result is a regulated world in motion: deregulation in some places, simplification in others, new guardrails elsewhere, and divergent speeds and approaches to policymaking.

Boards and senior management will need to assess how these complex political, economic and regulatory forces reshape their strategies and priorities. A clear risk appetite should steer strategic choices such as investment, technology selection, and operating models in this unpredictable environment. The importance of subsidiary boards is also expected to grow, as diverging global rules, geopolitical considerations, and distinct market conditions elevate the value of decisions taken at local levels. Opportunities will undoubtedly emerge, yet identifying and capturing them may be harder than usual.



The great regulatory recalibration – within limits

A familiar question is back with new urgency: can regulation protect consumers and stability without hindering innovation and growth? National competitiveness is an explicit political aim across many jurisdictions and regulators themselves may often be drawn in to support it. In response, there will be targeted deregulation rather than any wholesale rollbacks. The emphasis is on simplification and "right-sizing", although with regional variations in pace and methods.

The UK's Financial Services Growth & Competitiveness Strategy seeks to "rewire the financial system to boost growth", including reforms to consumer redress and bank capital policy.[2,3] Simplification, some of which amounts to targeted deregulation, is a core EU objective for 2026, with the Digital and Sustainability "omnibus" packages designed to streamline rulebooks. A similar dynamic is clear in the EU's Anti-Money Laundering agenda. By establishing a EU-level supervisor and moving to a single rulebook, policymakers are seeking to simplify a fragmented system, shifting the emphasis – at least in theory - to more consistent, proportionate and effective outcomes. While some simplification initiatives may lead to regulatory relief, it will likely be slow and selective. Overall, areas such as digital assets, operational resilience, and AI will likely attract more, not less, oversight.

In the US, the pendulum has swung more visibly, if selectively, towards focused rulemaking and supervision. Where new rules emerge (e.g., for stablecoins under the GENIUS Act), the aim is legal clarity and an accommodating posture.[4] Some states such as New York and California continue progressing with new rules, notably on consumer protection and the intersection of innovation (including AI), even as federal authorities shift towards refining, recalibrating, or reversing existing rules.[5] Divergence also persists across sectors - insurance specifically remains under significant supervisory pressure while new regulatory agency heads across banking and capital markets regulators are laying out their priorities and are expected to continue doing so. Whatever the policy direction, supervisory remediation will remain a central feature and, in some cases, may clear regulatory hurdles to further growth through organic expansion or acquisitions.

Asia Pacific (AP) authorities are favouring tactical streamlining and targeted interventions to remove duplication of regulations, especially for smaller firms, while taking a measured approach to the regulation of emerging technologies to balance innovation and risks.

For firms, the effects will vary. Some changes will ease balance sheet constraints, freeing capital and managerial bandwidth for growth initiatives. Others may cause burdens for international firms as "simplification" of and varying local approaches to regulations will likely yield diverging compliance requirements and IT changes across markets.

> *This [risk] outlook is increasingly characterised by hybrid risks that cut across financial, operational, technological and geopolitical domains*

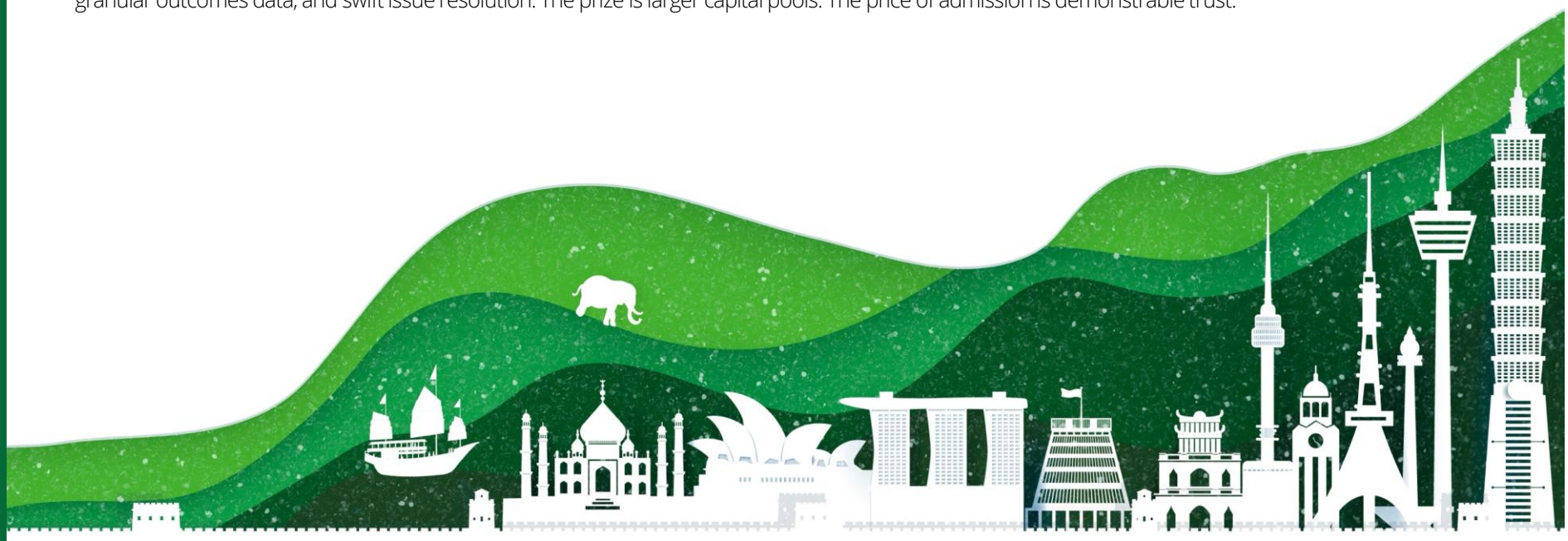
Mobilising retail savings - promise and prudence

Governments want deeper domestic capital pools to fund innovation, defence, infrastructure, and better retirement outcomes. With limited fiscal headroom, there is growing emphasis on harnessing retail savings to drive these critical investments.

The EU is pulling multiple levers to achieve these objectives. In particular, the Savings and Investments Union (SIU), aims to channel retail investment into productive assets, including via tax-advantaged investment accounts, and harmonise capital markets across the bloc.[6] The Retail Investment Strategy, aligned with the SIU, aims to safeguard and empower retail investors.[7] The UK is redrawing the advice–guidance boundary to enable "Targeted Support" to launch in 2026.[8] US policymakers are exploring broader access to private assets in retirement plans. Across AP, similar moves are underway to incentivise household investments in capital markets: Japan is expanding the Nippon Individual Savings Account, its tax-exempt retail investment programme, and Hong Kong SAR' s ("Hong Kong's") electronic Mandatory Provident Fund Platform is digitising pensions to cut fees and widen choice.

Yet, investment rhetoric is marching alongside rigorous consumer protection. In the UK, the Consumer Duty's fair-value tests and the motor-finance redress programme are reminders that distribution risk can quickly turn profits into significant costs.[9] The EU's retail package couples simpler investment journeys with tighter inducement and disclosure rules. Across AP, similar market-building and safeguarding measures are advancing in tandem, from anti-scam drives in Singapore and Hong Kong to design-and-distribution obligations and trustee accountability in Australia. The US continues to leverage existing guardrails, such as fiduciary duties for pensions and investment managers, and established enforcement practices, including at the state level.

Globally, strategies that take advantage of retail inflows must be inseparable from product-governance discipline: clear propositions, fair value evidence, granular outcomes data, and swift issue resolution. The prize is larger capital pools. The price of admission is demonstrable trust.



Private credit – booming, but casting long shadows

As policymakers encourage savers to invest, including in private markets, the supervisory spotlight is shining more brightly on the sector. Private credit is now a global force, with global assets under management reaching ~$2.5trn in 2025.[10] In the US alone, the market has grown from ~$46bn in 2000 to ~$1trn in 2023.[11,12] In comparison, the AP market remains smaller, but has nevertheless increased more than six-fold over the last decade.[13] Europe's private credit market has also expanded significantly, reaching €0.43trn in 2024, up from €0.15trn in 2014.[14]

This explosive growth is prompting supervisors globally to demand greater visibility – on valuation, leverage, liquidity, and interconnectedness with the wider financial system – in this largely bilateral, opaque market. Andrew Bailey, Bank of England (BoE) Governor and Financial Stability Board Chair, recently noted that US corporate collapses carry worrying echoes of the Great Financial Crisis. He highlighted the resurgence of familiar, risky practices – tranching and complex loan warehousing – while the BoE Deputy Governor for Financial Stability also raised concerns over weak underwriting standards.[15] In the UK, the BoE has launched a system-wide exercise to map vulnerabilities.[16]

A focal point for regulators everywhere will be understanding the multi-faceted ties between private markets and banks, insurers, and pension funds. This includes scrutinising the reinsurance mechanisms that transfer long-dated liabilities into less transparent assets. The UK has set supervisory expectations to limit links between funded reinsurers investing in private credit and UK insurers.[17] Bermuda now requires prior approval for long-term block deals and stronger liquidity guardrails.

AP authorities are signalling a similar shift in approach. In Australia, supervisors are pressing boards of superannuation funds to strengthen valuation governance and stress-testing practices. The Australian Securities and Investments Commission's (ASIC) 2025 review of private credit markets flagged opaque fee structures, conflicts, and confusing terminology. New guidance and a roadmap of Australia's approach to implementing the results of this review was released by ASIC in November 2025.[18]

The US regulatory stance on private credit has shifted significantly. The current administration, diverging from its predecessor's focus on enhanced data collection, largely attributes the sector's growth to regulatory constraints on traditional banking. While acknowledging that the sector warrants monitoring, new federal regulations remain improbable, absent a systemic crisis.[19] This contrasts with intensifying state-level scrutiny of life insurers, where the National Association of Insurance Commissioners is actively pushing for greater transparency, disclosure, and weighing the need for enhanced regulatory capital.

Global supervisory scrutiny of private markets, particularly private credit, will likely intensify through 2026. This will specifically target banks, insurers, and pension funds active in the sector, demanding robust evidence of their risk identification, management, and data aggregation capabilities. Yet, firm-level oversight alone risks obscuring system-wide vulnerabilities, making system-wide stress tests crucial.

> *While some simplification initiatives may lead to regulatory relief, it will likely be slow and selective*

The tower of Basel?

In our view, the fracturing global consensus is increasingly evident in the evolution of bank capital standards. The Basel framework, once the capstone of post-crisis cooperation, is firmly in the political crosshairs. The US has delayed its "Endgame" implementation, with a re-proposal expected in H1 2026 alongside separate proposals for further changes to global systemically important bank surcharges, stress tests, and enhanced supervisory leverage ratios.[20] The ripple effects are global.

The EU and UK have already deferred implementing the Fundamental Review of the Trading Book (FRTB) until January 2027. The UK is now consulting on a further delay to 2028 for implementation of the FRTB's Internal Models Approach, while the EU may adopt relief measures for FRTB which could significantly limit any increases in market risk capital requirements until January 2030.[21,22]

Basel implementation elsewhere also varies. Switzerland and Canada have fully adopted the standards. In contrast, the AP region remains fragmented: China (Mainland) ("China"), Japan, Hong Kong, and Singapore have fully implemented, while Australia remains a partial adopter, having delayed FRTB and Credit Valuation Adjustment implementation. Elsewhere, progress in other emerging economies is slower.

The substance of what will emerge in the US is as uncertain as its timing. If US rules are re-scaled, how far might they diverge from the agreed Basel standards? Should the US ultimately decline to implement FRTB, jurisdictions yet to implement will likely pause, while those that have implemented will face difficult decisions about how to proceed. For bank boards, this complicates capital planning and strategic capital allocation. The practical answer is scenario-based capital planning across multiple regulatory paths, plus strategic optionality based on business mix, footprint, and market participation.

More fundamentally, delayed and inconsistent implementation places the original purpose of the Basel framework (i.e. strengthening global financial stability through robust, risk-sensitive capital requirements) under strain. Fragmentation also risks introducing new systemic vulnerabilities and creating openings for regulatory arbitrage.

It also raises broader questions about how governments, central banks, and regulators might react to future global shocks, from private credit stress to major operational incidents. While a globally coordinated response, as seen during the Global Financial Crisis, remains the central case, it should not be taken for granted. Firms in their scenario testing may increasingly need to consider the implication of a shock resulting in disjointed, potentially conflicting, national interventions. Regulators may be contemplating similar scenarios and, consequently, may press local or regional entities to operate more autonomously, thereby creating redundancies across areas such as funding, liquidity, and IT systems.

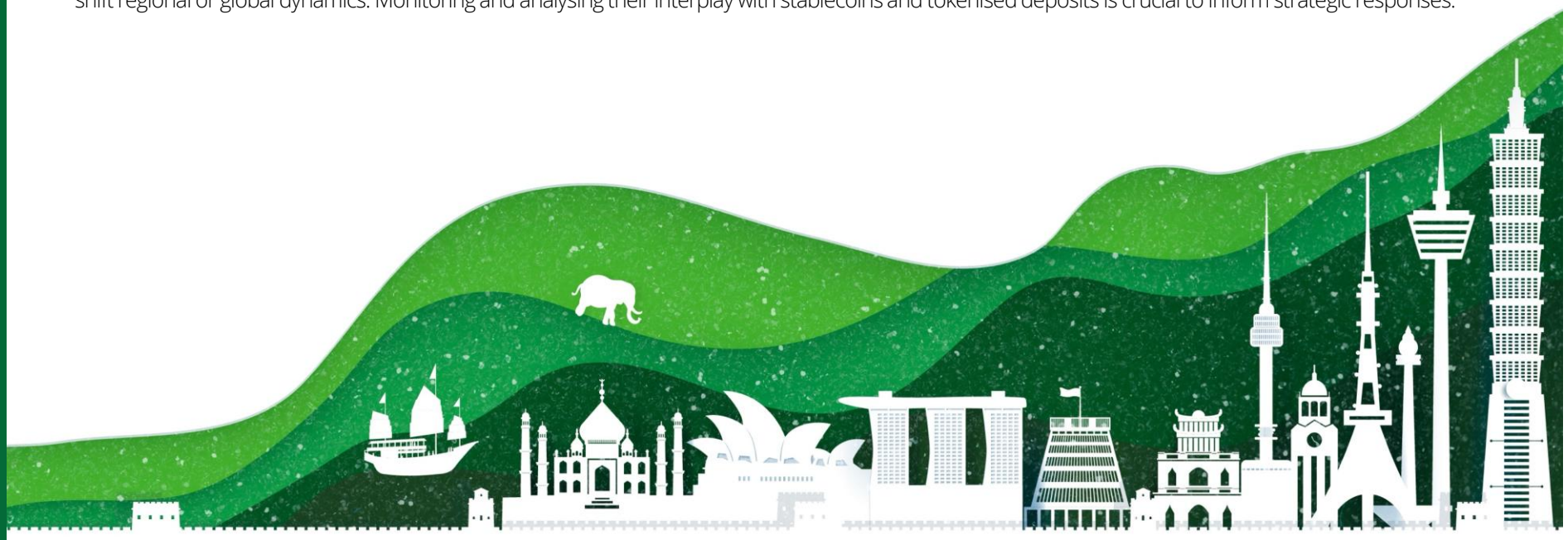
Digital assets – from edges to mainstream

Digital assets and blockchain technologies are transforming both the investment and payments landscape. On the asset side, we see continued efforts to harness these innovations to streamline securities issuance, trading, and settlement, enabling fractional investment and thereby improving access for retail investors. Yet this year, we expect the main step change to be on the payment side, with stablecoins and tokenised deposits emerging as industry priorities, driven by the promise of faster, cheaper, and programmable payments. Stablecoin issuance has surged and real-world use, though nascent, is growing. Strategic focus and legislative clarity in the US are catalysing a USD-dominated global market. The UK is accelerating in response, while Japan, Korea, Hong Kong, Singapore and EU regimes are already live, with local currency coins emerging across AP and Europe.

Tokenised deposits are advancing in parallel within existing banking rules, poised to coexist with stablecoins. Anchored on bank balance sheets, they offer lower counterparty and reputational risks - suited to corporates moving cash across subsidiaries or settling wholesale tokenised-asset transactions. Stablecoins, leveraging public blockchains, suit cross-border retail and business-to-business flows. The strategic prize is interoperability: seamless transition between the two could amplify adoption.

Two obstacles remain: domestic stablecoin regimes lack full clarity on their treatment of foreign-issued stablecoins or cross-border flows, and tokenised deposits mostly run on institution-specific rails, limiting scalability. Bank strategies could diverge. Universal banks may need capabilities in both instruments; corporate banks may favour tokenised deposits; retail and global payments players may prioritise stablecoins.

Retail central bank digital currencies, however, show more measured and mixed momentum, though progress in key jurisdictions (e.g., China and India) could shift regional or global dynamics. Monitoring and analysing their interplay with stablecoins and tokenised deposits is crucial to inform strategic responses.



Artificial intelligence – you can go fast, if you have the right guardrails

AI adoption shows no sign of slowing, although scaling and demonstrating clear returns remain key challenges. Policymakers, keen to foster innovation and growth, are expanding sandboxes and industry collaborations to support safe AI use. However, as adoption grows, 2026 will likely bring firmer supervisory scrutiny. As AI becomes more deeply embedded in core business processes and decision-making, supervisors will look for rigorous testing, comprehensive documentation, measurable outcomes, and board-level accountability. The AI agenda connects directly to operational resilience and the growing reliance on third-party providers, themes explored further below.

The EU AI Act will likely see its compliance deadline for high-risk systems extended by up to 16 months from its original August 2026 date.[23,24] This delay, necessary to finalise technical standards and provide regulatory clarity, offers firms breathing space, but no room for complacency. Financial supervisors in the EU and UK are also tightening scrutiny under existing and technology-neutral prudential, operational resilience, conduct, and accountability frameworks.

A critical gap remains: systemic and concentration risks stemming from foundation AI model providers are not yet fully captured by existing regimes. For now, firms should calibrate AI adoption strategies, set a clear risk appetite for exposure to these risks, and build governance that supports responsible experimentation and scaling within their risk tolerances.

In the US, AI regulations are decentralised with authorities at both the state and federal level issuing rules and frameworks for the technology. Federal initiatives, such as the proposed Unleashing AI Innovation in Financial Services Act, aim to spur adoption, but must contend with growing supervisory demands for governance and oversight.[25] States are moving too: Colorado's law for high-risk AI systems takes effect in 2026, while New York's Department of Financial Services has already issued guidance on third-party contractual controls, with further banking-specific directives anticipated.[26] States are moving too: Colorado's law for high-risk AI systems takes effect in 2026, while New York's Department of Financial Services has already issued guidance on third-party contractual controls, with further banking-specific directives anticipated.[26] Ultimately regulators across the financial sectors at the federal and state levels will continue to diverge in the short-term.

AP is equally diverse. Some jurisdictions are legislating, others are adapting privacy and cybersecurity frameworks or issuing AI guidance, reflecting different national security and innovation priorities. South Korea, for instance, is moving towards mandatory requirements for transparency, oversight, and risk-based obligations. Hong Kong and Singapore favour voluntary guidance. Singapore's Monetary Authority is promoting good practices and consolidating AI use cases, while simultaneously signalling a move towards stricter supervisory expectations.

Despite regional differences, regulators globally share a common goal: to foster innovation without diluting risk-based oversight. The core principle is that new capabilities, including Generative or agentic AI, must not override sound risk management. Firms can adopt AI quickly, provided they invest in essential capabilities and safeguards: a clear risk appetite, strong internal controls, robust risk management, and, crucially, accountability for outcomes.

> *The core principle is that new [AI] capabilities, including Generative or agentic AI, must not override sound risk management*

Operational resilience – efficiency meets reality

Operational resilience, including cybersecurity, is a board-level imperative globally. The rapid adoption of innovative technologies – such as AI, and looking further ahead, quantum computing - is amplifying the urgency. One particular concern for regulators worldwide is the growing concentration risks in critical digital infrastructure. These concerns also link to geopolitical shifts, prompting some countries to reduce reliance on cross-border AI, data, and technology stacks. This aims to strengthen supply chain resilience and lessen reliance on others. However, these efforts could also complicate global firms' efforts to build and maintain integrated resilience plans and scale and deploy AI systems across markets.

UK, EU, and Australian regimes were fully embedded in 2025, with stricter supervision looming. Hong Kong banks face a May 2026 deadline. In the US, federal banking agencies have long supervised third-party service providers, including technology providers, and US state authorities (e.g., New York) are also intensifying third-party risk scrutiny. Oversight of critical third parties in the UK (subject to their designation) and EU also commences in 2026.

Despite varying specificity from prescriptive EU rules to principles-led but exacting UK/Australian demands, frameworks converge on core capabilities: mapping services and dependencies, scenario testing, incident management and third-party governance. For cross-border groups, various regulatory demands often require replicating evidence, reporting, and operational playbooks, even where underlying capabilities are shared. Coupled with an ever-evolving threat landscape, operational resilience becomes a continuous endeavour.

Boards face a dilemma in vendor selection: major players offer superior tooling and economies of scale but concentrate risk. Diversification enhances failovers but raises complexity and costs. The key is to weigh disruption costs – financial, reputational, regulatory fines – against mitigation investments, treating resilience as a strategic capability.

Firms should ensure impact tolerances genuinely reflect customer expectations, validated through operational exercises to ensure issues are resolved or backed by remediation plans. Effective contingencies are essential, including the ability to access data when needed (e.g. through secure copies of information in other locations) and handle demand spikes. Multi-cloud strategies should provide genuine portability and failover capabilities. Crucially, aligning with supervisory expectations and engaging authorities early can help minimise potential costly setbacks later.

> *These [operational resilience] concerns also link to geopolitical shifts, prompting some countries to reduce reliance on cross-border AI, data, and technology stacks*

The regulatory landscape is undergoing a complex recalibration as authorities pursue growth and innovation amidst a challenging risk and geopolitical outlook. This profound shift involves deregulation in some areas and streamlined regulation in others. The result is a more fragmented regulatory and supervisory environment as authorities pursue their own objectives and global coordination recedes.

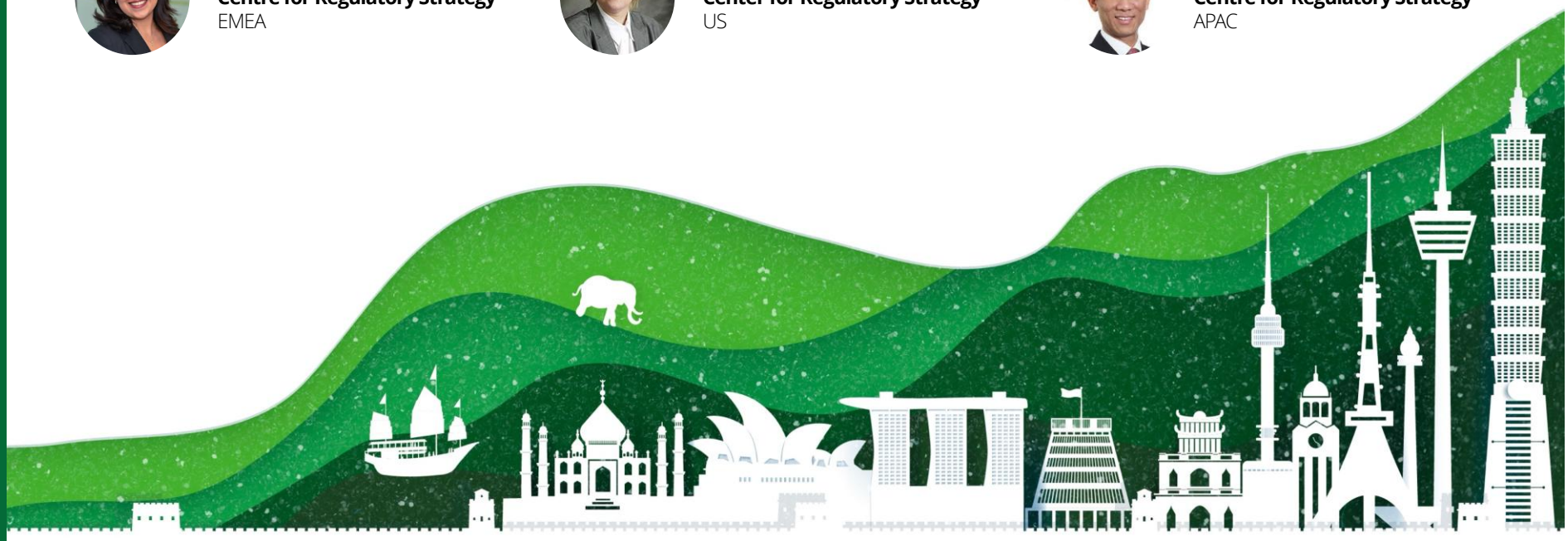
In parallel, novel risks are emerging or intensifying, from Generative and agentic AI and digital assets to operational resilience and geopolitical challenges. While new regulations aim to address some areas, others will likely see increased supervisory focus. This confluence of global regulatory divergence, rapidly evolving risks, and shifting supervisory expectations will make the landscape more complex for firms to navigate. Still, boards and senior management should also consider the opportunities these shifts create, capitalising on the growth and innovation governments aim to stimulate. As firms respond, the growing importance of subsidiary boards will require governance frameworks that ensure local decisions align with group-wide aims, even as local regulatory and market conditions vary.

Against this backdrop, risk appetite takes an ever more important guiding role. Firms need to have a full appreciation of the scale, complexity, and trajectory of future risks, and clarity on the boundaries within which they intend to compete, innovate, and invest. Proactively defined risk boundaries and tolerances should guide key decisions, including on investment, pricing, technology, partnerships, product design, and market entry or exit, rather than merely controlling outcomes retrospectively.

Suchitra Nair
Centre for Regulatory Strategy
EMEA

Irena Gecas-McCarthy
Center for Regulatory Strategy
US

Nai Seng Wong
Centre for Regulatory Strategy
APAC



Asia Pacific Perspective

Asia Pacific (AP) enters 2026 with momentum and resilience, supported by continued investment and the region's depth of demand.

Yet the external environment remains highly fluid. Trade policy is again a decisive swing factor, including the risk of renewed or higher tariffs and related countermeasures which could reconfigure supply chains, cost bases and export demand across key AP markets. Alongside this, conditions remain uneven across the region and funding markets continue to shift, keeping boards focused on balance sheet discipline, liquidity and the ability to respond quickly as growth, inflation and capital flows diverge.

Against this backdrop, two forces will define the next phase of the regulatory and risk agenda more than any single macro variable: rapid technology acceleration and persistent geopolitical uncertainty. Geopolitical competition is increasingly extending into data, cloud services and the AI infrastructure required to build and operate advanced models. As a result, the push for "sovereign AI" - a country's ability to develop, deploy and govern AI in line with domestic laws is accelerating. National security, resilience, and self-sufficiency are key drivers, particularly where AI capability underpins critical services and sensitive data processing.

Across financial services, AI is moving from limited pilots to a core capability across front-, middle-, and back-office functions. Supervisors now expect firms to demonstrate they can scale the technology safely through clear accountability, robust controls and a mature approach to model risk management across the organisation. At the same time, rapid advances in AI are remaking the financial crime landscape. Criminals are weaponising AI to industrialise scams and social engineering, accelerate identity misuse and mule recruitment, and conduct adaptive, cross-channel attacks. Concurrently, stablecoins and other forms of digital money are becoming embedded in payments and market activity. Firms will face faster, more complex cross-border flows and new typologies for fraud, money laundering and sanctions evasion, often spanning both traditional and digital-asset rails across AP.

Further, geopolitical fragmentation is shrinking the scope for a single global operating model. As national requirements diverge on data access, outsourcing and technology sourcing, firms will need to increasingly tailor their local operations to meet local regulatory requirements. Meanwhile uncoordinated policy is making it harder to achieve effective collaboration across borders. This has the potential to slow collective action on fast moving challenges such as AI enabled financial crime and digital asset related illicit flows, while increasing complexity for firms operating across multiple jurisdictions. Divergent regimes can also create opportunities for regulatory arbitrage, as activity (and risk) migrates towards jurisdictions with less mature or less consistently enforced rules.

For the *AP FSI 2026 Regulatory Outlook*, we have focused on *Artificial Intelligence & Technology, Digital Assets* and *Financial Crime* because they sit at the nexus of accelerating innovation, tighter supervisory expectations and heightened geopolitical uncertainty. Developments in one area now directly shape the others, as AI rewires decision making; digital assets transform how value moves and markets function; and financial crime adapts to exploit both. Taken together, the chapters provide a connected view of some of the key priorities that will occupy firms, regulators and supervisors in 2026 and beyond.

In Focus

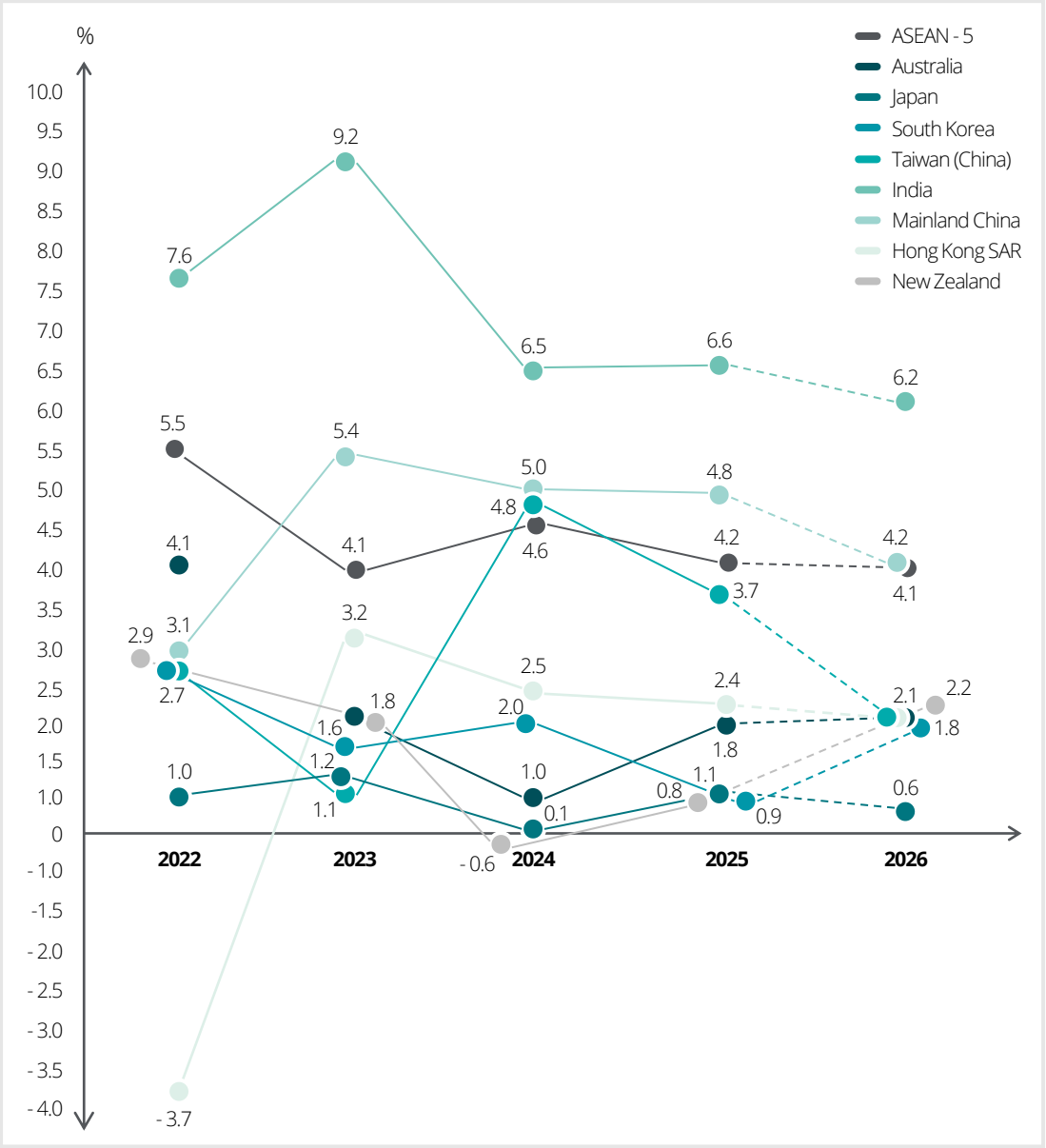
Macroeconomic Environment

Resilience amid shifting trade patterns

The AP region faced historically elevated uncertainty at the start of 2025 as the US announced punishingly high tariffs on its exports. At the time, it was expected that growth would be severely hampered since many export-oriented economies in the region rely heavily on the US market. However, with the year now in the rear-view mirror, it is evident that the region outperformed these grim expectations. This resilience was enabled by a combination of tariff pauses that led to export frontloading, trade carveouts, and supportive domestic policies.

But some of the tailwinds that propped up growth in 2025, particularly on the trade front, have likely run their course. In 2026, it is expected that the broader reorganisation of global trade will become clearer. Tariffs in the US, more stringent environmental policies in the EU, and uncertain domestic demand in parts of AP may present challenges due to excess industrial capacity. Geopolitical tensions in the region, could also reassert themselves and pose economic risks.

The outlook also includes opportunities over the longer-term. Trade reorganisation, the global AI investment boom, and the green energy transition could each benefit a wide range of economies in the region, while a growing consumer base in India and other parts of Southeast Asia could help the AP region become more resilient. However, the possibility of an AI investment bubble and a potential slowdown in the green transition due to geopolitical tensions present risks. The IMF expects the AP region to grow slower compared to previous years.[27] Despite the slowdown, the region is projected to account for 60% of global growth in 2026.[28]



Near-term challenges and risks are likely to slow growth in 2026

Slower growth in global trade

The frontloading of orders and a sharp increase in AI investment boosted trade volumes in 2025. These factors resulted in the World Trade Organisation (WTO) raising its forecast for growth in global trade volume in 2025 from 0.9% to 2.4%.[29] However, relatively strong growth in trade is unlikely to be sustainable, especially as tariffs imposed by the US come into full effect. This may be further compounded by tighter enforcement against "transshipment", as authorities move to curb routing of goods that are re-routed to obscure their true origin through other economies. The WTO forecasts global trade volumes will grow just 0.5% in 2026.[30] This tariff-induced slowdown is expected to weigh on the AP region's export-oriented economies. The region's exporters will also have to contend with the European Union's (EU) Carbon Border Adjustment Mechanism (CBAM) which will come into effect in 2026 and impose additional costs on carbon-intensive exports.[31] The EU is also set to impose stringent anti-deforestation measures in late 2026 and through 2027.[32] These measures could weigh on Indonesia's and Malaysia's palm oil exports. Consumer confidence in China remains low which reflects weak domestic spending in the world's second largest economy.[33] Overall weaker global demand for the AP region's exports could force producers in the region to cut prices, putting pressure on profits and the sustainability of some businesses.[34]

Changing trade patterns

As trade barriers introduced by the US come into full effect in 2026, global trade is also likely to be redirected. Moreover, traders will have to contend with a renewed focus on national resilience and security, with the ongoing de-risking of US and China supply chains at the core of this trend. These developments could pose a risk to large parts of the AP region that are reliant on China as a supplier and on both China and the US as major markets. Economic risks will rise if countries are forced to choose sides between the world's two largest economies.

At present, the ASEAN countries are also experiencing a surge in exports from China. This trend is likely to continue as China redirects exports away from the US and as its domestic market remains subdued. This trend could weigh on small and medium-sized enterprises in the AP region, potentially resulting in job losses and business closures. If pressures mount and countries in the region choose to put up protectionist barriers against these imports – such measures could slow global trade further.

China's economic trajectory

More generally, slowing, and unbalanced economic growth in China is a key risk as it is the primary destination for the AP region's exports. Some of China's economic challenges are structural – an overreliance on investment has resulted in very high debt levels at the local government level and across state-owned enterprises. Excess industrial production and relatively weak consumer spending have resulted in China becoming increasingly reliant on exports. In 2025, China's trade surplus exceeded $1 trillion for the first time.[35]

The prolonged downturn in the country's residential real estate sector, due to a combination of overinvestment, a government crackdown on debt, and a shrinking population, is likely to continue to weigh on consumer sentiment and overall growth in 2026 as the real estate sector accounts for 70% of household wealth.[36] Domestic science and technology is likely to be a bright spot as the push for self-reliance continues.

Longer-term opportunities will keep the region attractive

Threading the needle on trade

The outlook also includes opportunities, even amid a complicated trade environment. For instance, the ASEAN economies could benefit from cheaper intermediary imports from China, especially if the bloc's exports gain market share in the US and Europe where China's exports face relatively higher barriers. Research indicates that ASEAN countries have benefitted from pro-growth foreign direct investments from China while significantly gaining market share in the US in recent years. However, solidifying this trend would require the bloc to thread the needle, including by boosting the domestic content of its exports to the US market.

The AI boom

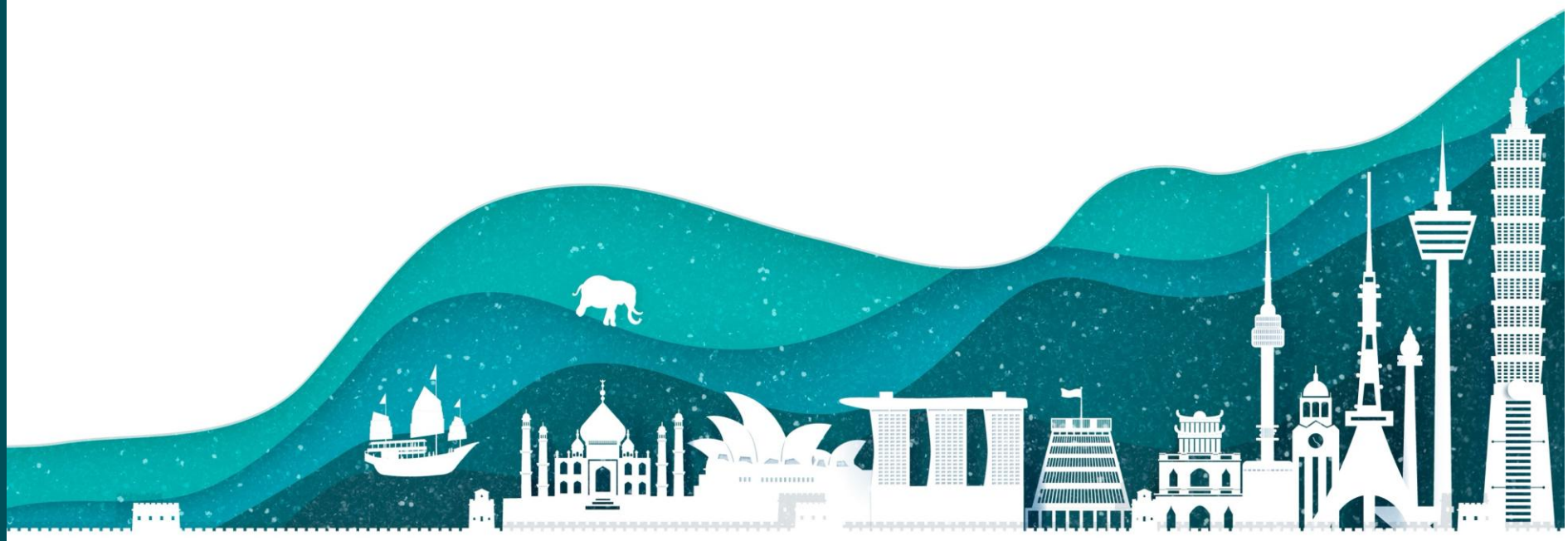
Strong investment in AI infrastructure is likely to continue across the global economy in the near term, led by developments in the US. This trend is expected to support strong demand for semiconductors and electronics manufactured in economies such as Taiwan (China) ("Taiwan"), South Korea, and Japan. Benefits could also spill over to jurisdictions such as India where technology services exports could gain as AI adoption expands across the global economy. Malaysia is harnessing the AI boom and is considered to be developing data centre capacity faster than any other AP jurisdiction.[37] Extensive investment in AI-related infrastructure is also likely to boost demand for financial services. More broadly, the World Trade Organisation (WTO) projects that if AI boosts productivity and lowers costs, the value of global trade in goods and services could increase by as much as 40% by 2040. The AP region is well-positioned to capture a significant share of this value because of its manufacturing expertise. However, despite the promise of significant productivity gains, the adoption of AI at scale within enterprises has lagged the rapid investment in infrastructure, therefore leading to some fears of overinvestment. This gap between capital deployed and realised returns has fueled debate over whether parts of the current cycle risk overheating. Elevated valuations, concentrated investment in infrastructure providers, and uncertain monestisation models raise the prospect of repricing if growth expectations are not met. For AP economies heavily exposed to semiconductor and data-centre supply chains, any slowdown in AI investment could have spillover effects on exports and credit conditions.

The green energy transition

Investment in renewable sources of energy such as wind and solar and in green technologies such as electric vehicles and energy storage is likely to grow over the coming years in line with government mandates around environmental goals. The growing demand for solar panels and wind turbines as well as critical minerals such as lithium, nickel and cobalt will benefit several countries in the region. China is uniquely placed to play a pivotal role in the global transition given its dominant role in green energy technologies and in the processing of critical minerals for the energy transition. Other countries in Southeast Asia with well-developed manufacturing industries and countries with natural endowments of critical minerals such as Australia and Indonesia are also well positioned to gain from a pivot to green energy. Trade in green energy products and technologies within the AP region is expected to accelerate, especially as a growing share of the region's economy comes under pressure due to climate change. This trend is also likely to support demand for green finance.

Growing consumer base

The AP region's vast consumer base is projected to expand rapidly. This is likely to be driven by rapid growth in India and Southeast Asia. It is estimated that consumer spending in Southeast Asia alone could exceed that in North America by 2035.[38] This growing consumer base will offer the AP region a counterbalance against possible slowing growth in China. Intra-regional trade is likely to make the AP region more resilient to external shocks from other parts of the world. However, simmering intra-regional tensions could pose a threat to this narrative.



Key themes for the financial services industry through 2026

Continued technological disruption will present opportunities and pose challenges

In AP, financial services firms are likely to witness ongoing technological disruption from the implementation of AI and other technologies such as quantum computing. Such technologies could boost productivity by improving operational efficiency, increasing transaction velocity, and potentially transforming business models and engendering new products and services. Payments connectivity, already supported by bilateral and multilateral schemes to connect payment operators, could be enhanced further by technology implementation. Modern technologies will also enable measures to deter frauds and scams. The number of fintech providers could increase off the back of technological advancements. Increased competition from fintechs could squeeze profit margins among traditional financial services providers, forcing them to innovate. The increased digitalisation of financial services is also likely to keep the focus on cyber security and operational resilience across the industry.

Regulatory measures are likely to evolve in response to technology adoption

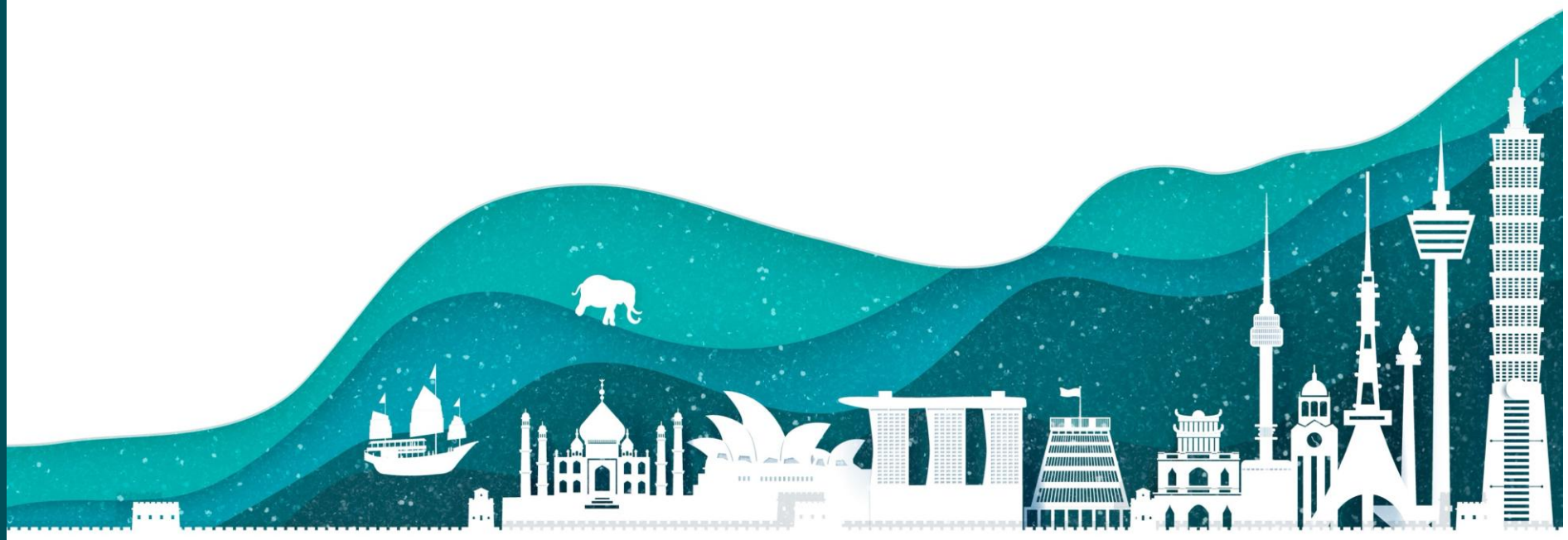
Financial services firms are likely to see regulatory measures evolve in response to technology adoption. In general, AI-related regulation is expected to take shape across the region. Regulators are also expected to make operational resilience a key focus as cyberattacks grow in scale and sophistication. At the same time, geopolitical and national security considerations are increasingly influencing authorities' view of AI and cloud as critical infrastructure. In several markets, this is translating into stronger emphasis on sovereign AI and the resultant policies designed to retain domestic control over critical AI infrastructure. Authorities are seeking greater control over where sensitive data is stored and processed, how models are trained and accessed, and the degree of reliance on a small number of global cloud platform and foundational model providers (and the compute supply chains that underpin them). For financial institutions, supervisory expectations could therefore extend beyond general third-party risk management towards explicit jurisdictional and vendor "assurance". Firms will need to evidence where key AI capabilities sit, what legal and operational controls apply, and how firms would maintain continuity if access is constrained by geopolitical shocks, policy shifts or provider outages. This may bring increasing scrutiny of portability, and exit planning for critical AI-enabled services, as well as a strong emphasis on local capability building in order to reduce strategic dependence. Further, Fintechs could come under greater regulatory oversight as they become more critical to the industry. Regulators are also likely to continue focusing on digital payment security and countering frauds and scams, particularly in markets where digital payment volumes are growing rapidly.

Demographic patterns are expected to create opportunity

Financial services firms will see a range of demographic patterns playing out over the near term in the AP region. In South Asia and Southeast Asia, rapid income growth and continued urbanisation is likely to bring a larger share of the population under the umbrella of financial services. More developed parts of the AP region where populations are relatively older and wealthier are likely to see a significant transfer of wealth. It is estimated that more than 60% of the region's high-net-worth individuals are over 60 years of age.[39] However, the absence of formal succession planning could pose a risk and present an opportunity to financial services providers.[40] This gap increases the risk of contested transfers, governance breakdowns and forced asset sales., potentially heightening default probability during periods of market stress. For financial institutions, this also creates a sustained demand for structured succession planning, trust services and balance sheet solutions.

Uncertainty is expected to remain elevated

Businesses have been operating in an environment of heightened uncertainty over the past few years. This environment is broadly expected to continue as multiple factors including geopolitical tensions, technological developments, resource scarcity, and climate change patterns overlap one another. Firms must therefore plan for uncertainty as the baseline and build resilience, optionality, and the ability to adapt at speed into theirs operating models.



Top three actions for financial services firms in 2026

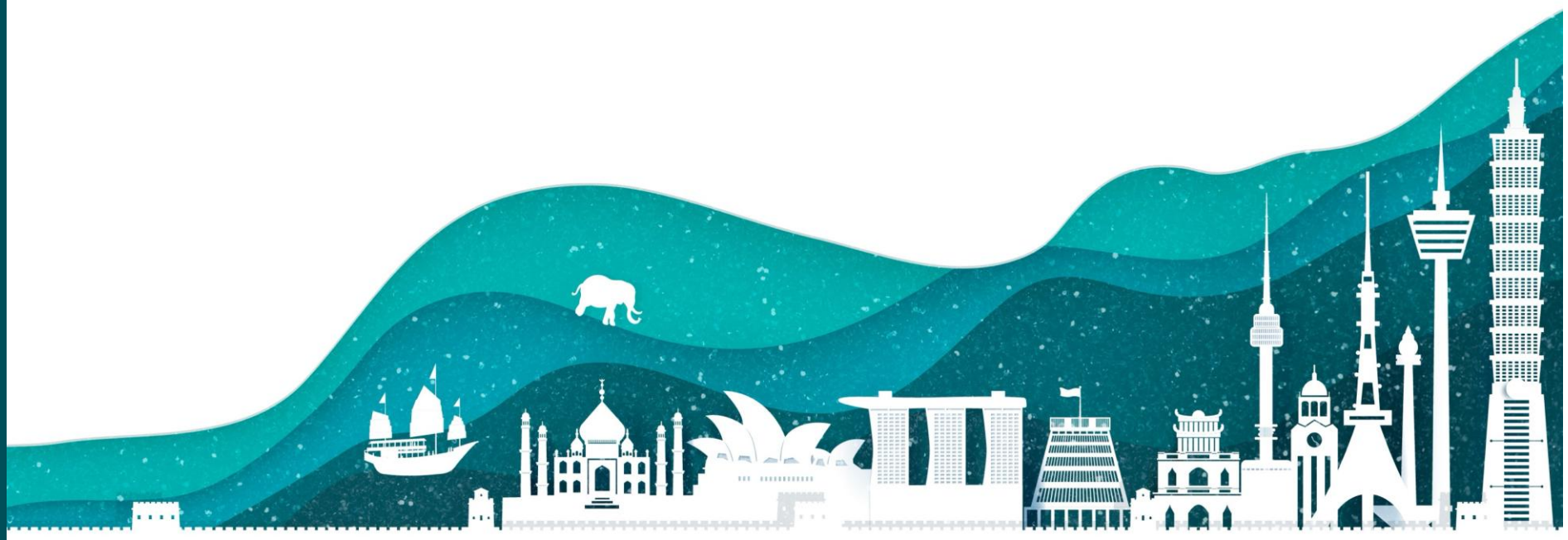
Invest in geopolitical sensing
Geopolitical developments have become a crucial factor in business decisions. It is therefore critical that financial institutions build up their ability to anticipate and pre-emptively adapt to geopolitical changes. Investing in geopolitical sensing will enable FS firms to stress test their operations based on potential scenarios.

Enhance cyber resilience
The proliferation of AI and the development of quantum computing could result in a higher cyber security threat to the FSI. Cyber criminals have adopted a 'harvest now decrypt later' approach whereby they collect and store data that can be decrypted at a later stage using quantum computing and AI. In general, technology-enabled fraud and attacks tends to outpace developments in security. To remain resilient, it is therefore critical that FS firms invest in enhancing cyber resilience.

Monitor economic developments closely to stay agile
Firms should monitor the various economies in the region as economic paths diverge. Broadly, economies in North and East Asia are expected to grow at a slower pace than those in South Asia. Inflation outlooks are also varied. For instance, inflation in Japan has remained historically high and some degree of inflationary pressure has reemerged in Australia. It is broadly expected that these geographies will experience slower price growth in 2026, although a sustained weaker yen could keep import costs elevated and make inflation more persistent than expected. Meanwhile, inflation in other parts of the AP region could accelerate from a low base after being dormant in 2025. In general, monetary policy is expected to remain supportive across the region with room for further easing. However, some central banks are likely to remain more hawkish. Monetary policy in the US and subsequent short-term interest rate differentials will influence currency valuations and capital flows. The Bank of Japan's normalisation of policy interest rates could contribute to some degree of volatility in currencies and longer-term interest rates across the region. As interest rates rise in Japan, a considerable flow of Japanese capital could be repatriated, resulting in weaker domestic currencies and higher long-term interest rates.

In summary, the AP region is likely to stay relatively resilient in 2026. However, as temporary tailwinds weaken, growth in the region is likely to slow during the year. Near term risks are likely to be dominated by tariffs in the US and the redirection of global trade. China's imbalances and economic slowdown are likely to be a drag on the AP economy. And geopolitical tensions are expected to exert an influence over the region's economic prospects.

The AP region's longer-term opportunity to capture a larger share of the global exports market while tapping into the AI boom and the green energy transition are expected to keep it attractive to global investors. Favourable demographics and rapid growth in South Asia and Southeast Asia are expected to boost domestic demand and contribute to greater economic resilience.



Artificial Intelligence & Technology

AI adoption at an inflection point

AI uptake accelerated across AP in 2025 as more financial institutions moved beyond pilots towards wider deployment. However, progress remains uneven and continues to depend on each institution's risk appetite, the maturity of its technology foundations, and broader strategic priorities. Outcomes are also highly dependent on the quality and availability of data, with weak data foundations continuing to limit performance in many firms. At the same time, geopolitical frictions and data sovereignty considerations are accelerating interest in "sovereign AI" – more localised deployment of modules, compute and controls to keep sensitive data within jurisdictions and reduce reliance on a narrow set of offshore platforms. For financial institutions, this is beginning to reshape cloud and vendor choices, cross-border deployment patterns and third-party risk management expectations.

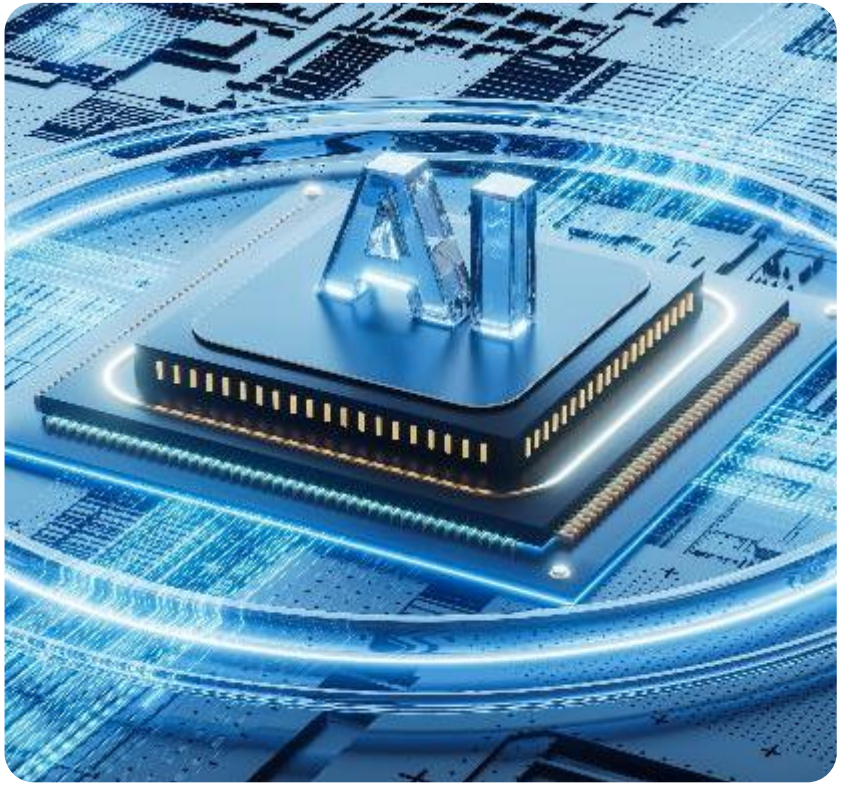
The shift from experimentation to scaling AI use cases into full production remains challenging, particularly in large, complex organisations where resistance to change and incremental delivery mindsets can slow adoption. Further, the operational effort required to prepare and govern data, redesign processes, and manage risks, can in some instances, outweigh near-term gains.

Firms are also contending with the challenge of model drift, where model performance degrades over time due to changes in data, user behaviour or operating conditions. This is increasing the need for continuous monitoring and periodic re-validation rather than reliance on point-in-time testing at deployment.

Against this backdrop, progress increasingly hinges on workforce capability. Sustained investment in training, upskilling and AI literacy across business, technology and risk is needed. This will give firms the confidence to pursue more ambitious use cases, redesign end-to-end workflows and translate AI advances into measurable productivity and service improvements.

Meanwhile, AI capabilities continue to advance at pace. Developments in multimodal systems and more autonomous or 'agentic' AI are expanding the range of potential use cases and improving system reliability and usability. Introduced appropriately, these advances may help to reinvigorate enthusiasm for AI deployment, particularly where newer capabilities are less resource-intensive and integrate more seamlessly within an organisation.

Authorities and FIs are also beginning to look beyond AI deployment to adjacent technology shifts that could reshape the risk and governance landscape. Quantum computing is emerging as a potential enabler of more powerful optimisation and analytics supporting AI-enabled advances in areas such as risk modelling, fraud, detection & decisioning. At the same time, it could weaken the encryption that underpins secure data-sharing, digital identity and transaction integrity, necessitating early readiness planning and targeted investment to stay ahead of bad actors.



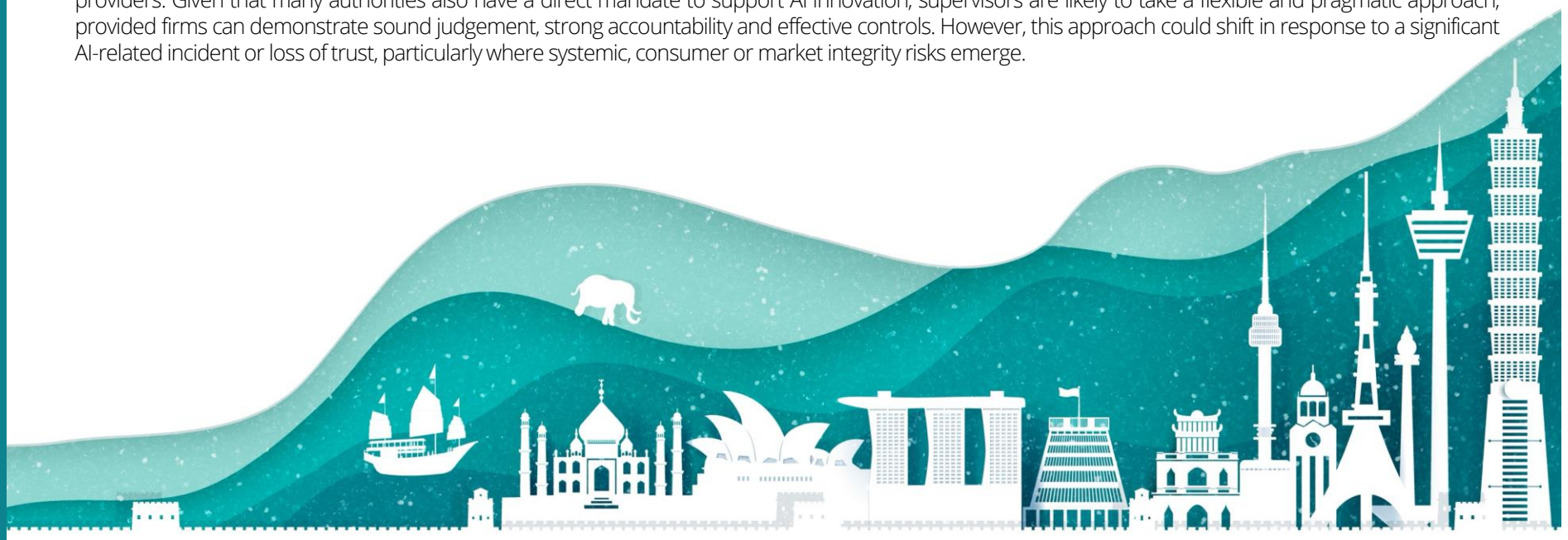
A complex and fast-moving regulatory landscape

2025 saw a marked increase in the volume of AI-related reports, consultations and initiatives across the AP region. In most jurisdictions, regulators continue to rely on existing technology-neutral legal and supervisory frameworks, such as those relating to cybersecurity, data privacy, and workplace discrimination. However, at the pan-industry level, several AP authorities are introducing, or consulting on, mandatory requirements for high-risk or high-impact AI, reflecting a broader global shift towards risk-based regulation.

Regardless of approach, authorities across AP are increasingly aligned around a common set of risk concerns. These include accountability and oversight; fairness and transparency/explainability; data quality and privacy; safety; security; and third-party dependencies. For financial institutions, this evolving landscape sits alongside a mature and robust regulatory environment. AI use cases, including credit scoring, insurance claims, transaction monitoring, and financial advice, will be assessed primarily through prudential and model risk management standards, conduct obligations, and operational resilience requirements. As a result, Financial institutions can expect increasing supervisory scrutiny of how AI is governed and controlled in practice, even in the absence of AI-specific requirements, or where they remain principles-based and non-binding.

Looking ahead to 2026, supervisory focus is expected to intensify on firms' AI strategies, governance arrangements and risk-management practices, particularly for large and systemically important financial institutions. FSI supervisors are looking to boards and senior managers to understand the risks and ensure that they are comfortable with the trade-offs between the risks and rewards inherent in AI adoption.

Attention is also likely to centre on high-risk AI used in material, customer-facing or decision-critical activities, as well as dependencies on key third-party providers. Given that many authorities also have a direct mandate to support AI innovation, supervisors are likely to take a flexible and pragmatic approach, provided firms can demonstrate sound judgement, strong accountability and effective controls. However, this approach could shift in response to a significant AI-related incident or loss of trust, particularly where systemic, consumer or market integrity risks emerge.



Pan-industry regulatory developments

Across AP, we are seeing continued momentum in the development of AI policy frameworks, with a growing number of jurisdictions moving from high-level principles towards more concrete, and in some cases legally binding, regulatory regimes. While approaches differ, most authorities continue to favour risk-based regulation, with requirements calibrated to the risk classification and potential impact of AI systems and use cases.

South Korea

In South Korea, the AI Framework Act will enter into force in January 2026, introducing mandatory requirements for 'high -impact' and generative AI.[41] In the second half of 2025, the Ministry of Science and ICT (MSIT) began consultation on a draft Enforcement Decree, setting out how the framework will work in practice. The draft decree provides greater specificity on delegated elements of the Act, including definitions of high-impact and GenAI; transparency and user-notification requirements; safety and risk-management expectations; and processes for determining whether systems fall within scope. The Act also provided for the establishment of South Korea's AI governance architecture in late 2025, including a national AI policy/strategy committee and supporting institutional bodies (such as AI safety and policy centres) to underpin standard-setting, guidance and supervisory coordination as the requirements moves into implementation.

Vietnam

Vietnam passed a long-anticipated AI Law in December 2025, which sets out a four-tier risk framework with phased implementation beginning in March 2026.[42] It prohibits unacceptable use cases and imposes strict obligations on 'high-risk' systems, including risk assessments, human oversight, model registration, and incident reporting. 'Medium risk' systems face transparency requirements with voluntary standards for 'low risk' systems. The Law also sets baseline expectations for general purpose models and those deemed to pose systemic risk including requirements for technical documentation, cybersecurity measures and enhanced testing.

Thailand

Further, after a two-year pause, Thailand restarted its legislative process issuing its own draft AI law.[43] High-risk AI face obligations around risk assessments, human oversight, incident reporting and documentation, with a requirement for offshore providers to appoint a local legal representative. Under the proposal, rather than mandate a fixed list of prohibited or high-risk AI in primary legislation, risk classification would be delegated to sector-specific regulators.

Taiwan (China)

In January 2026, the Taiwan Artificial Intelligence Basic Act entered into force, with the aim of promoting AI innovation while managing risks through a tiered governance approach.[44,45] The Act is grounded in seven widely recognised AI governance principles: sustainability and well-being; respect for human autonomy; privacy and data governance; cybersecurity and safety; transparency and explainability; fairness and non-discrimination; and accountability. It also promotes privacy-by-design, includes protections related to labour rights and introduces labelling requirements for high-risk AI applications including appropriate warnings. For high-risk uses, the government will also define liability and responsibility conditions and put in place mechanisms for remedies, compensation, or insurance. The National Science and Technology Council (NSTC) has been designated as the lead authority; however, the Act does not immediately impose compliance obligations on the private sector. The Ministry of Digital Affairs (MODA) will be responsible for developing a risk-classification framework aligned with international standards. Sector regulators will then use this classification to implement risk-based regulations, including the ability to restrict or prohibit harmful AI applications. The Act also mandates the establishment of a "National AI Strategy Special Committee" to coordinate national AI affairs.

China (Mainland)

In China, GenAI 'Labelling Rules' came into effect in September 2025, which mandate both explicit and metadata-level identification of AI-generated content.[46] Alongside this, three national standards on GenAI security[47], data annotation[48] and training datasets[49] came into effect in November 2025. The standards require firms to evidence strong controls around training data sourcing, traceability, annotation quality, model-security safeguards, access management, and monitoring.

Japan

In Japan, the AI Promotion Act came into full effect in September 2025, and represents a significant step to establish a legal framework for the development and application of AI technologies.[50] However, the AI governance remains under a "soft law" approach. The Act is primarily a policy-driven initiative designed to foster innovation, advance research and development, and promote responsible use of AI technologies. AI governance requirements remain non-binding, with the Ministry of Internal Affairs and Communications (MIAC) and Ministry of Economy, Trade and Industry (METI) leading on the development of iterative pan-industry guidelines for business, last updated in April 2025.

Australia

Conversely, Australia appears to have stepped back from an earlier proposal to introduce mandatory guardrails for high-risk AI systems, releasing a national plan in December 2025 that relies on voluntary industry frameworks rather than enforceable obligations.[51] The government also indicated that it intends to use existing privacy, consumer and sectoral laws to govern AI. This follows the release of new Guidance for AI Adoption ("GfAA") in October 2025, which replaced the Voluntary AI Safety Standard (the "VAISS").[52] The new guidance has been framed as a response to industry feedback, as well as rapid shifts in technology and the governance landscape over the past year. GfAA streamlines VAISS's ten guardrails into six core practices for both developers and deployers, and takes a more prescriptive, lifecycle-wide approach across development, deployment, and ongoing evaluation. The National AI Plan will also establish the AI Safety Institute (AISI), whose role will be to monitor, test and share information on emerging AI capabilities, risks and harms. The AISI aims to support regulators in maintaining safety measures, laws and regulatory frameworks that keep pace with technological change.

India

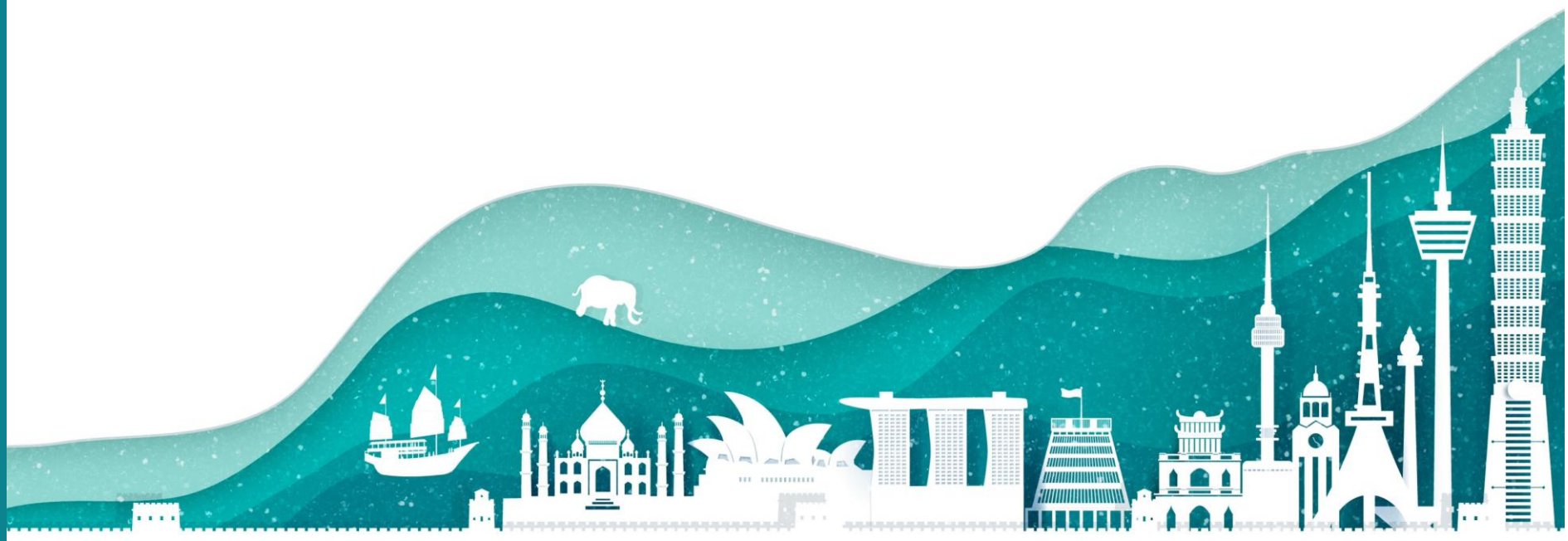
India seems to be taking a similar approach. The country's AI Governance Guidelines, released in November 2025, signal a principles-based non-prescriptive approach to AI regulation with a focus on sectoral regulators providing oversight of domain-specific risks.[53] The Guidelines set out seven cross-sector principles aimed at supporting responsible innovation while promoting trust, accountability, safety and resilience. India has also indicated that AI risks will be addressed primarily through targeted amendments to pre-existing legal and regulatory frameworks, rather than through new prescriptive rules. This includes clarifying how existing data-protection requirements apply to AI, such as the use of personal data for training models, purpose limitation, and the role of consent managers in AI-driven processing.

New Zealand

New Zealand also continues to take a light-touch, principles-based approach to AI regulation, relying primarily on existing technology-neutral laws such as the Privacy Act and Commerce Act rather than introducing AI-specific legislation. Current policy direction centers on voluntary guidance, most notably the Responsible AI Guidance for Businesses , which encourages firms to adopt transparency measures and determine proportionate levels of human oversight based on the risk profile of each AI system.[54] Reflecting New Zealand's preference for distributed governance, AI oversight spans multiple agencies including the Privacy Commissioner and the Government Chief Digital Officer, alongside a range of economic, foreign affairs, public-sector and competition/ consumer protection bodies supported by cross-government coordination forums. While not prescriptive, this framework signals an expectation that businesses remain accountable for AI-enabled decisions and ensure responsible development and deployment practices as AI adoption accelerates across sectors.

Singapore

Singapore's pan-industry approach to AI regulation remains collaborative and experimentation-led, prioritising voluntary standards, regulatory sandboxes and public-private pilots to build trust and inform future governance. The AI Verify Foundation, together with the Infocomm Media Development Authority (IMDA), launched the Global AI Assurance Pilot in February 2025, involving participation from six FIs and FinTech firms.[55] The initiative aims to support the development of common testing norms for GenAI, build trust through greater transparency around AI performance, and inform the evolution of both open-source and proprietary AI testing tools. Early findings published in May 2025 highlight that effective AI testing should focus on the most significant risks for each use case, rather than applying generic testing approaches. Standard or off-the-shelf test data is often insufficient, meaning firms need to plan and budget upfront for sourcing or creating suitable test data (including difficult edge-case scenarios) drawing on both engineering effort and subject matter expertise. The findings also note the value of reviewing both interim system behaviour and final outputs, with appropriate levels of human oversight remaining important even where AI is used to scale evaluation. Based on participant feedback, potential future focus areas include training; standardisation of testing approach; developer accreditation schemes; and scalable test environments with democratised access to testing technologies. Further, recognising the additional and amplified risk presented by AI agents, in January 2026, IMDA launched a Model AI Governance Framework for Agentic AI.[56] The guidelines emphasise the need to evaluate risks early and set clear limits as well as establish strong controls and clearly defined processes. The report further highlights the importance of maintaining meaningful human involvement and accountability; and enabling end-user responsibility through transparency and training initiatives. IMDA are also working with firms to collect information on case studies and to understand how organisations are currently approaching governance and risk management of agentic AI.



Financial services supervisory expectations

Across AP, financial services regulators have been clear that AI will be supervised primarily within the existing regulatory rulebook, rather than through new AI-specific regimes. Supervisory focus has therefore centred on how firms are operationalising AI governance and risk management in practice, supported by a strong emphasis on collaboration with industry through guidance, reviews and sandbox initiatives.

Australia

In Australia, ASIC indicated that it does not intend to rush into new AI-specific regulation, emphasising that existing, technology-neutral laws already provide important guardrails for the safe and responsible use of AI. ASIC also cautioned that overly prescriptive regulation risks adding complexity and compliance burden, potentially diverting resources away from innovation and productive outcomes, and signaled that it will continue to enforce existing obligations as they apply to AI-enabled activities.[57] APRA similarly stated its view that AI can be managed within existing prudential and conduct frameworks, while noting that it will step up monitoring of AI-related risks at larger institutions. This includes reviewing the appropriateness of risk management, governance and oversight arrangements.[58]

Japan

In Japan, the Financial Services Agency (JFSA) issued a discussion paper in March 2025 also indicating its current preference to supervise AI under existing laws and regulations. The report focussed on surveys and AI use cases, highlighting common industry challenges including those related to data such as availability, quality, security and personal information protection; and third-party risks of external vendors.[59] On GenAI specifically, explainability, bias and hallucination were discussed; as well as challenges relating to model risk management and testing, where the importance of taking a risk-based approach was emphasised. The JFSA has also signalled plans to publish follow-up guidance including governance and risk management best practice around March 2026.[60]

Hong Kong SAR

In Hong Kong, the authorities continue to prioritise innovation sandboxes and industry collaboration enabling firms to test AI use cases in a controlled environment. In October 2025, the Hong Kong Monetary Authority (HKMA) published practical insights from its ongoing "GenA.I. Sandbox initiative" which focusses on the use of AI in risk management, anti-fraud measures, and enhancing customer experience.[61] The report covered data strategy and preparedness; solution design including model selection and validation; and discussed risks relating to explainability, hallucination, bias, security and privacy. The HKMA also indicated that future sandbox work will focus on embedding AI governance across the three lines of defence, strengthening proactive risk management, including the use of AI to monitor AI, and introducing adaptive guardrails and self-correcting mechanisms.

Malaysia

Malaysia also continues to emphasise collaborative supervision, using a regulatory sandbox approach.[62] In August 2025, Bank Negara Malaysia (BNM) published a discussion paper clarifying that AI use remains subject to existing technology-agnostic, outcomes-focused regulatory frameworks.[63] The paper emphasised supervisory expectation that firms implement proportionate, lifecycle-based AI risk management, with particular focus on governance, data management and the protection of personal data. BNM also signalled that supervisory attention may increase if AI-related risks become more material, are used in critical functions or to replace human decision-making. Looking ahead, BNM has indicated that potential future work includes developing industry-led guidelines and best practices for AI risk management and governance; facilitating knowledge-sharing on AI implementation and validation techniques; strengthening AI talent and leadership capabilities within the sector; and enhancing consumer awareness to build trust in AI-enabled services.

Singapore

In Singapore, this collaborative stance is being complemented by a gradual codification of supervisory expectations as AI use matures within the FSI. In November 2025, the Monetary Authority Singapore (MAS) consulted on new Guidelines for AI Risk Management which build on MAS' earlier thematic reviews of AI use in banks and information paper on AI model risk management.[64] The draft guidelines outline supervisory expectations for governance, risk-tiering of AI use cases, lifecycle controls (including data quality, testing, monitoring and change management) and the organisational capabilities needed to deploy AI safely. MAS also emphasised proportionality and the need for firms to align AI oversight with the materiality of each use case. The proposed guidelines are complemented by an AI Risk Management Executive Handbook issued at the same time by the Project MindForge industry consortium.

New Zealand

In New Zealand, supervisory agencies have reinforced that AI will be governed through existing regulatory requirements rather than new AI-specific rules. The Reserve Bank of New Zealand (RBNZ), in its May 2025 Financial Stability Report, highlighted that institutions must identify, assess and mitigate AI-related risks as part of their broader risk-management, governance and operational-resilience frameworks.[65] This has been reinforced by the Financial Markets Authority (FMA), which in August 2025 highlighted AI as a priority area, particularly in credit underwriting, pricing and capital allocation and stressed that AI outputs must be reliable, explainable and contestable, with strong safeguards for sensitive data.[66] Regulators remain supportive of innovation, including through the FMA's regulatory sandbox and its broader reviews of tokenisation and emerging technologies – but have been clear that firms must embed AI governance within existing prudential, conduct and data-protection obligations. As AI use matures, regulatory engagement is likely to deepen, with heightened scrutiny for use cases that pose elevated risks or involve automated advice, credit decisions or large-scale customer interactions.

From policy to practice

Emerging best practice points to the importance of strong overarching governance and controls, combined with use-case-specific model design and risk management.

Governance approaches are still evolving. Some firms have decentralised ownership across business units and legal entities, while others centralise decision-making within a head office function. More mature firms are largely adopting a hybrid approach: a group-wide framework for AI governance with delegated authority to implement models within pre-defined guardrails. This allows for tailored and flexible deployment while also ensuring a consistent view of risk and controls. Additionally, we have observed that where governance primarily sits – technology/data versus the risk function – often influences both the pace of AI adoption and the rigour of testing and independent challenge. This reinforces the need for a balanced approach that enables innovation while maintaining effective risk management.

Across AP, FSI supervisors will increasingly expect AI governance to be embedded in enterprise-wide governance and risk frameworks. Firms should show clear roles and responsibilities, and lifecycle controls that cover intake, change, and ongoing monitoring.

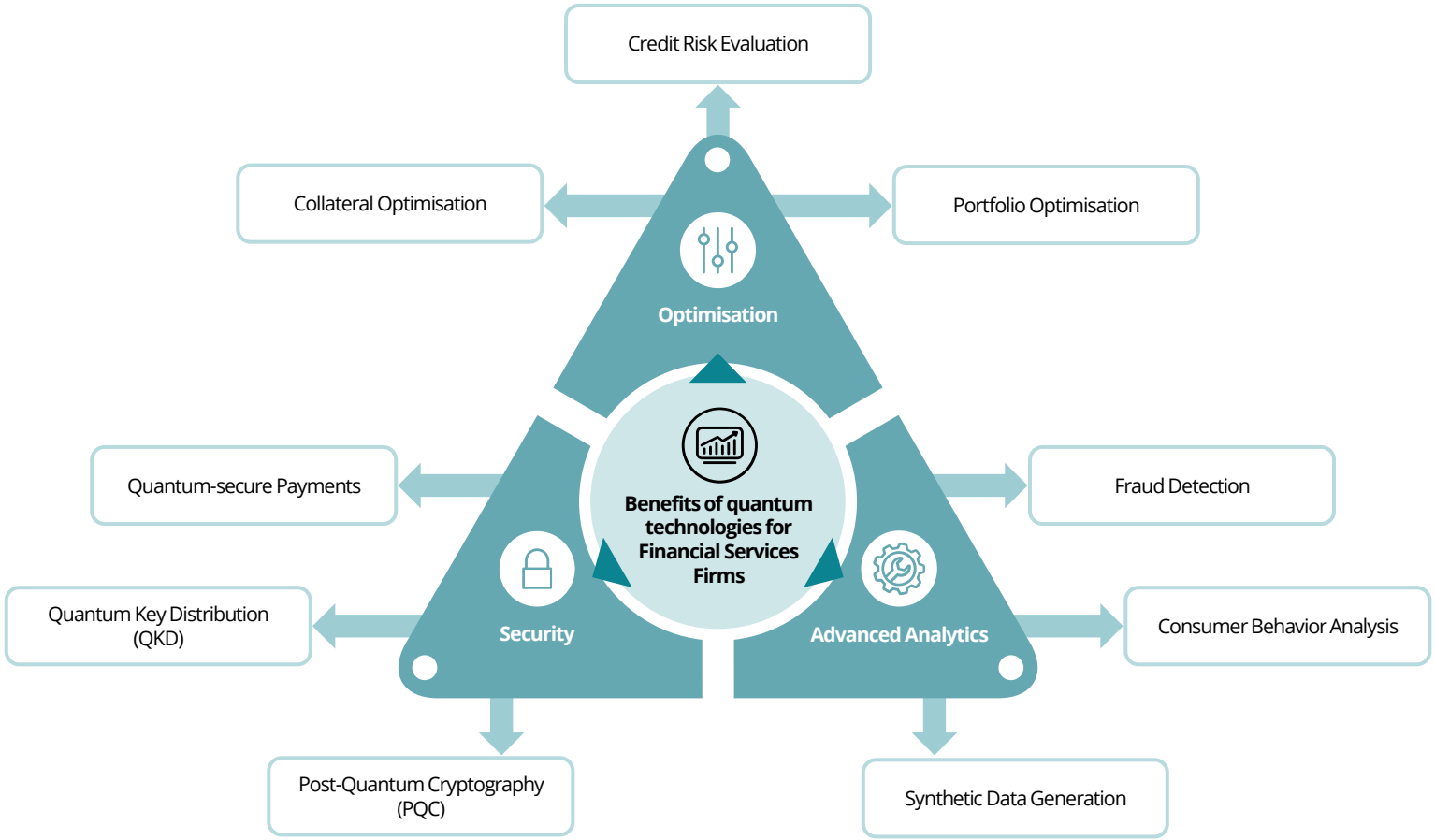
Boards and senior executives will be expected to set a clear, actionable AI risk appetite and demonstrate active oversight. The risk appetite should define where AI can be used, acceptable levels of autonomy, and rules for testing, monitoring, and reporting. Executives need an up-to-date view of all AI deployments, the materiality of each use case, and reliable management information (MI) on performance, incidents, limitations, dependencies, and emerging risks. Decision rights and escalation paths should be well understood and supported by technology-enabled workflows where appropriate with playbooks that enable rapid intervention when issues arise, including pausing or rolling back systems if needed.

Expectations will also center on proportionate, risk-based oversight. Firms should implement risk tiering and a taxonomy that distinguishes low-risk productivity tools from customer-facing applications, high-impact decisioning models, and more autonomous agent capabilities. Controls must scale with risk: lighter oversight for low-risk, low-impact AI, and more rigorous validation, explainability, documentation and security for more critical systems. Supervisors will expect decision makers to demonstrate they understand model risks and limitations, can explain and manage uncertainty in outputs, and can evidence reliable, fair, and consistent outcomes.

Supervisors will also expect to see evidence of strong collaboration between business, technology, data, and risk teams, appropriate resourcing and skills, and a culture that embeds AI risk management across the organisation.

Quantum technologies

Quantum technologies apply the principles of quantum mechanics to solve problems beyond the abilities of classical computer systems, particularly those involving huge numbers of possible outcomes.[67] For the FSI, the most relevant early use cases include faster optimisation (e.g., portfolio and balance-sheet decisions), improved analysis of very large datasets, and new approaches to securing sensitive information. While adoption is still at an early stage, leading institutions are already testing pilots to understand where quantum could deliver advantages and where it may introduce new cyber and resilience risks. Quantum is also increasingly viewed as complementary to AI given that many AI applications ultimately depend on complex optimisation and pattern-finding, and quantum techniques may improve the speed or quality of outcomes for specific workloads. In parallel the move to post-quantum cryptography (PQC) will be important to protect the data that AI models rely on.



Quantum computing has significant potential to transform the FSI. Potential applications include:

Quantum computing providing more accurate risk modelling and fraud detection;

Quantum security capabilities such as quantum key distribution (QKD) and quantum random number generation (QRNG);

Quantum capabilities to further reduce the latency of high-frequency trading algorithms.[68]

Quantum security capabilities such as QKD and QRNG are particularly significant developments for financial institutions and regulators seeking to enhance security in financial services communications networks. As firms rely more on cloud services and external data centres, they are increasingly dependent on complex, interconnected networks to transmit and store sensitive information. This has become a growing area of concern to regulators in the region, and quantum technologies such as QKD and QRNG are being explored as a potential enhancements to existing security controls – particularly for links between financial institutions and third-party infrastructure.

The MAS has been at the forefront of regulatory interest in the capabilities of QKD. In 2024, MAS launched a proof-of-concept sandbox in collaboration with financial and technology industry partners to explore the use cases of QKD in the financial services industry.[69] MAS issued its technical report following the culmination of the sandbox exercise, finding that QKD has the potential to significantly enhance the security of communication networks, particularly those between financial institutions and data centres.[70]

Some regulators in the region are also concerned about the threats that quantum computer-enabled malicious actors might pose in the future. The Chief Executive of the HKMA announced as part of its "Fintech 2030" strategy that industry readiness for post-quantum cryptography (PQC) is an area of focus.[71] This is the process of developing algorithms resistant to attacks from quantum computers. In Australia, the Australian Signals Directorate released updated guidance on planning for PQC with indicative timelines for firms to implement their readiness plans.[72] The JFSA raised PQC as one of its main topics of concern in a dialogue with the Japan Securities Dealers Association in June 2025.[73]

Quantum computing technology has significant potential to enable financial institutions to enhance the security of their communications networks in an increasingly digital and cloud-based environment. It also has the capability to enable malicious actors to conduct more sophisticated and damaging criminal activity. The challenge for regulators and financial institutions going forward will be harnessing the potential of this technology whilst simultaneously understanding and planning for its hostile use against them.

Key trends to watch in 2026

Continuous Monitoring

AI systems can behave differently once deployed as data, users and operating conditions evolve, and performance can degrade in ways that are not anticipated at go-live. Ongoing monitoring and validation is therefore essential to detect drift and unexpected outputs early, and to ensure that AI continues to operate within agreed guardrails. Firms will need to define and monitor risk and quality indicators to ensure that AI is operating safely and securely. This should include signals of inappropriate or harmful outputs, emerging bias, unexplained volatility, abnormal input or output patterns, and potential data leakage. When these signals are detected, escalation and investigation should be immediate, with clear ownership for remediation through tech-enabled standardised workflows where appropriate. Risk and quality indicators need to be available both at a granular level and rolled up to reliable Management Information (MI) for executive and board consumption.

Scaling Human Oversight

Many firms remain in a largely "human-in-the-loop" (HIL) phase, where a person reviews or approves AI-supported decisions before they are executed. This can provide strong assurance, but it is resource-intensive and can become a bottleneck as AI use expands. Some leading firms are starting to move toward "human-on-the-loop" (HOL) oversight, particularly for lower risk use cases. HOL allows AI to act within agreed boundaries, without pre-approval for every decision or the need to review every output. Control comes through automated checks and validations (often AI-enabled) that continuously test whether outcomes stay within pre-approved guardrails.

Supervisors increasingly recognise that HIL models can constrain scaling. However, they will want to see evidence that HOL is robust, including whether decision rights are clear, escalation works in practice, and issues can be contained quickly.

Managing external dependencies

Many FIs are integrating vendor capabilities directly into workflows rather than building and operating all components in-house. In 2026, supervisors are expected to increase scrutiny of how institutions assess, monitor and mitigate the risks associated with these third-party dependencies. This will increasingly include where critical AI capabilities sit, including reliance on offshore model providers, cloud infrastructure and embedded AI services and whether firms can evidence appropriate jurisdictional assurance and resilience. Supervisors are also concerned about rising concentration and systemic risk given that there are a small number of AI platforms/ model provider and cloud vendors, increasing the risk of widescale outages, cyber incidents or service degradation.

A growing focus will be on transparency over third-party capabilities, particularly the data used to train or fine tune models, the methods used to build and evaluate them, as well as the controls and security measures being put in place. Supervisors will look for mitigants to vendor and geographic concentration risk, including portability, exit planning and continuity arrangements for AI-enabled services deemed critical.

Supervisors will also expect firms to have credible contingency plans for critical AI-enabled processes. Financial institutions will therefore need to strengthen outsourcing and vendor risk management frameworks to reflect AI-specific considerations, including clear service boundaries, change-notification rights, and requirements for ongoing performance and risk monitoring.

Navigating data constraints

Data sovereignty and localisation rules are increasingly shaping how firms design and deploy AI. Across the region, supervisors are tightening expectations on where sensitive data is stored and processed, how it can be transferred, and what controls are required when processing data offshore. In 2026, these constraints will continue to influence technology architecture, cross-border operating models and even vendor selection. As a result, firms may need to demonstrate that AI training, inference and monitoring can be executed within required jurisdictions (or with appropriate safeguards), rather than relying on cross-border data movement as the default. Firms will need credible data-flow mapping and cross-border assessments, backed by controls proportionate to the sensitivity of data.

More broadly, data privacy and permissible data use in AI training will continue to be key focus areas. Supervisors will expect clear discipline over what personal or confidential data is used in AI. As discussed in our recent paper on Safeguarding Data Privacy in AI, "privacy by design" will be increasingly important, for example, ensuring data use is minimised and anonymised as much as possible.[74]

Ensuring fairness and transparency

Supervisors recognise the potential for AI to improve access and affordability of financial products, particularly for underserved segments, but they will expect firms to demonstrate that outcomes remain fair. Rapid AI adoption also raises the risk of consumer harm through opaque automated decisions, AI driven interactions, and technology amplified scams that exploit behavioural biases. Supervisors note uneven AI governance maturity across firms and the increasing risk that autonomous systems propagate errors and misconduct at scale.

Conduct will therefore remain a central supervisory focus as AI moves into front-line customer interactions and decisions. Expectations for outcome-based testing will increase, with supervisors looking for evidence of strong monitoring for unintended impacts, bias, inconsistent decisions or adverse outcomes, particularly for vulnerable customers.

Firms will also need to clearly disclose when customers are interacting with AI, implement controls to prevent misleading or manipulative communications, and ensure meaningful human involvement for high-impact activities (e.g., suitability assessments, pricing/credit-related decisions, and complaints handling). Where firms use AI to support these decisions, they should be able to explain why a result was reached in plain language, apply appropriate challenge, and ensure customers can obtain timely review and remediation.

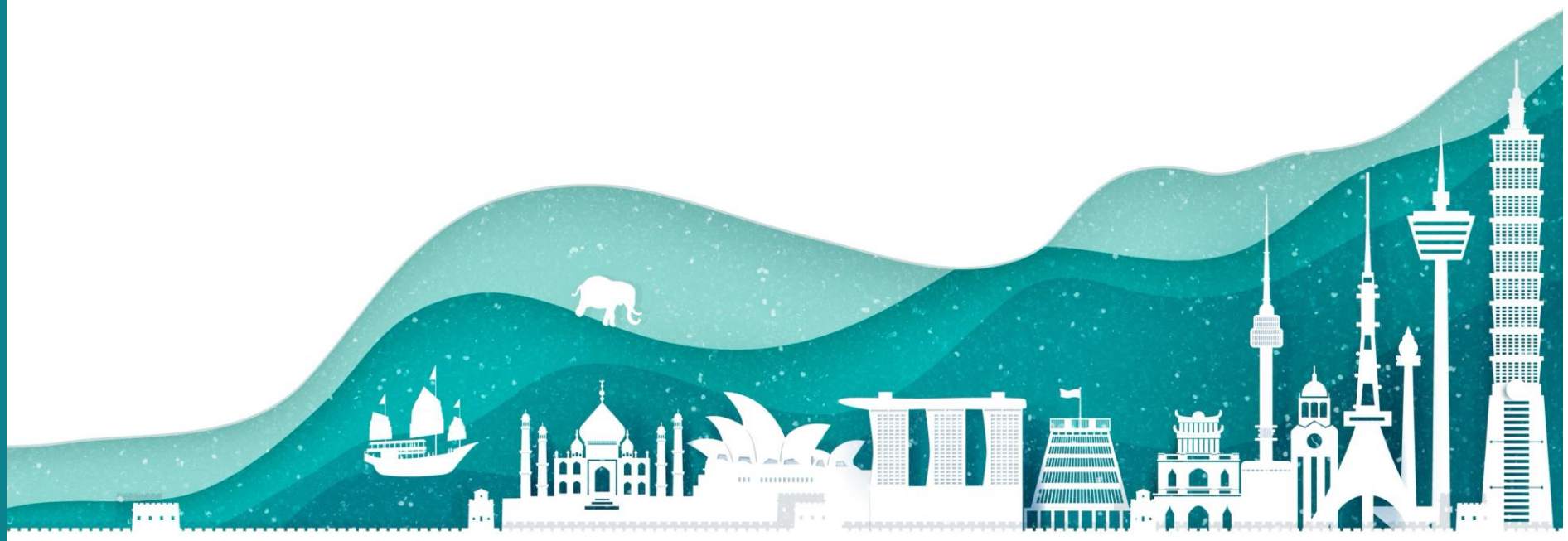
The rise of agents

Agentic AI can plan, decide and execute a sequence of actions to achieve a goal (often directing multiple systems). As AI models acquire greater autonomy, the supervisory focus will also need to consider containment and control. This means keeping actions within defined boundaries and preventing rapid error propagation across integrated workflows, particularly for multi-agent systems. In practice, agentic AI can act as a compounding risk factor: one misconfigured or misbehaving agent may influence others through chaining (where one agent's output becomes another's input), feedback loops, and shared dependencies across tools and data sources.

Firms will be expected to evidence controls over autonomous behavior including precise permissions and decision rights (what the system may execute autonomously, what requires human authorisation, and what is prohibited). Firms will also need to demonstrate they can quickly identify, isolate and shut down a misbehaving agent, and can switch to manual or rules-based alternatives when needed. The rise of agentic also presents challenges for scaling human oversight. While governance will likely shift towards "human-on-the-loop" supervision, "human-in-the-loop" will still need to be maintained for a limited set of predefined high-impact or irreversible actions ("chokepoints") where additional assurance is required.

As AI implementation moves from pilots into broader deployment, supervisors are likely to focus less on whether firms have policies in place, and more on how governance is being actioned in practice. That starts with clear board and senior executive accountability: a defined AI risk appetite, agreed boundaries for use, and decision rights and effective escalation routes.

To scale AI safely, firms also need strong foundations. In particular, supervisors will look for robust model risk management, strong data governance and operational resilience, supported by continuous model monitoring to detect drift, performance degradation and unintended outcomes over time.



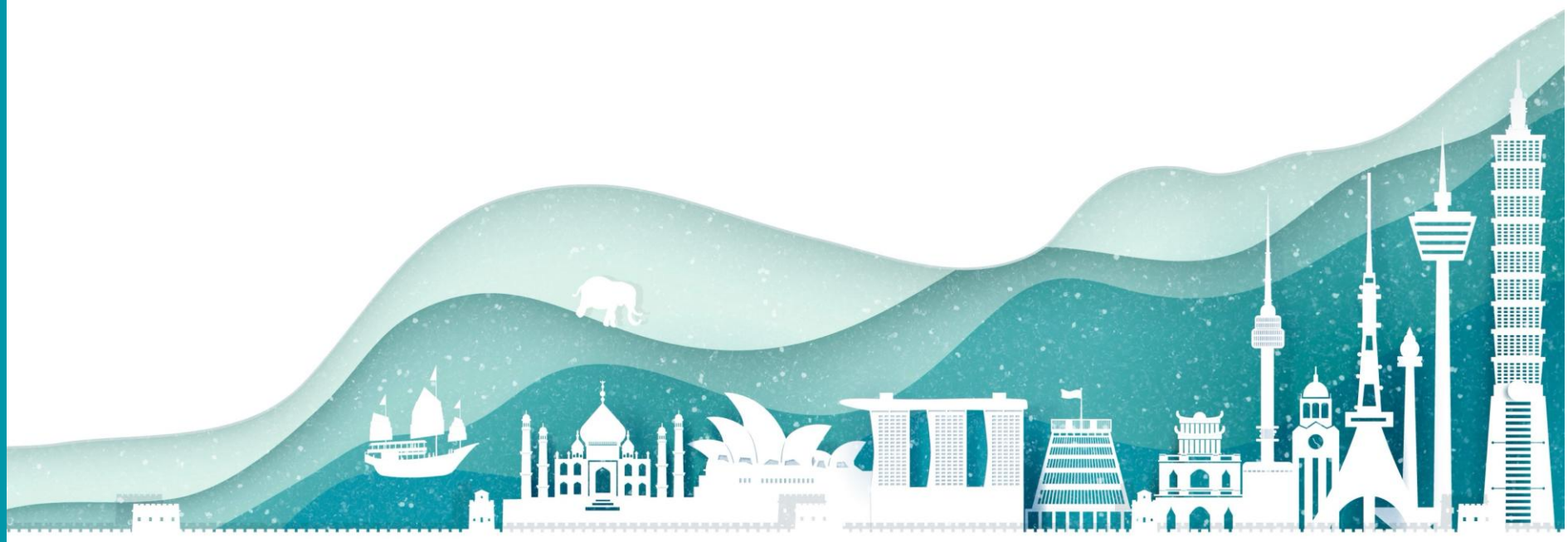
Digital Assets

Digital assets are fundamentally transforming AP's financial infrastructure, transitioning from experimental ventures to core components of institutional investment strategies and payment systems.

Accelerated adoption of cryptocurrencies, stablecoins, and tokenised assets is driving efficiency in cross-border settlements, enhancing liquidity, and enabling new capital market access.

Adoption of digital assets has exploded across the region with an estimated one in four adults using some form of digital asset in 2025.[75] This is likely driven by the proliferation of stablecoins and tokenised assets in emerging markets. The traditional financial centres of the region have also seen significant growth in the digital assets market, for example, Hong Kong saw a 233% YoY increase in digital asset trade volumes on Hong Kong exchanges in the first half of 2025.[76]

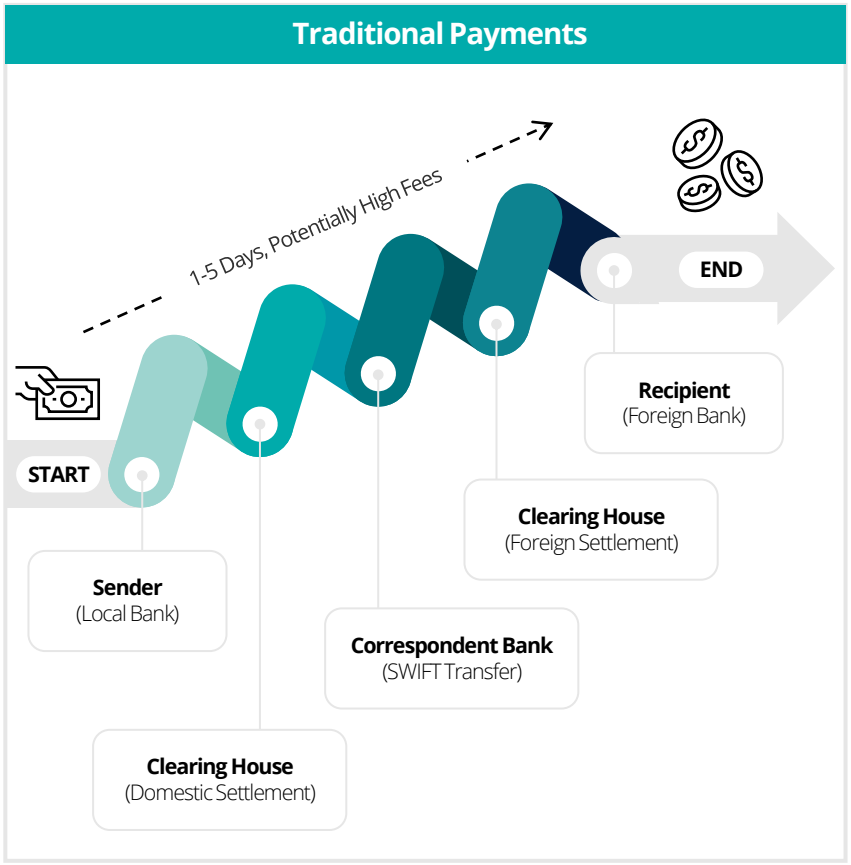
To provide regulatory clarity, authorities are introducing frameworks to address market abuse, investor exposure, and systemic risks. At the global level, the USA as the world leader in digital assets has introduced the Digital Asset Market Clarity Act of 2025 which is designed to communicate to the public how the government and financial regulators approach digital assets.[77] In AP jurisdictions including Singapore (MAS), Japan (JFSA), Hong Kong (HKMA and Securities & Futures Commission (SFC)) and Australia (ASIC) have set out their regulatory approaches which includes stringent licensing, custody requirements, and anti-money laundering protocols. As activity scales, supervisors are also sharpening expectations around market integrity and conduct, with stronger scrutiny of disclosures, marketing and end-to-end client asset protection arrangements.

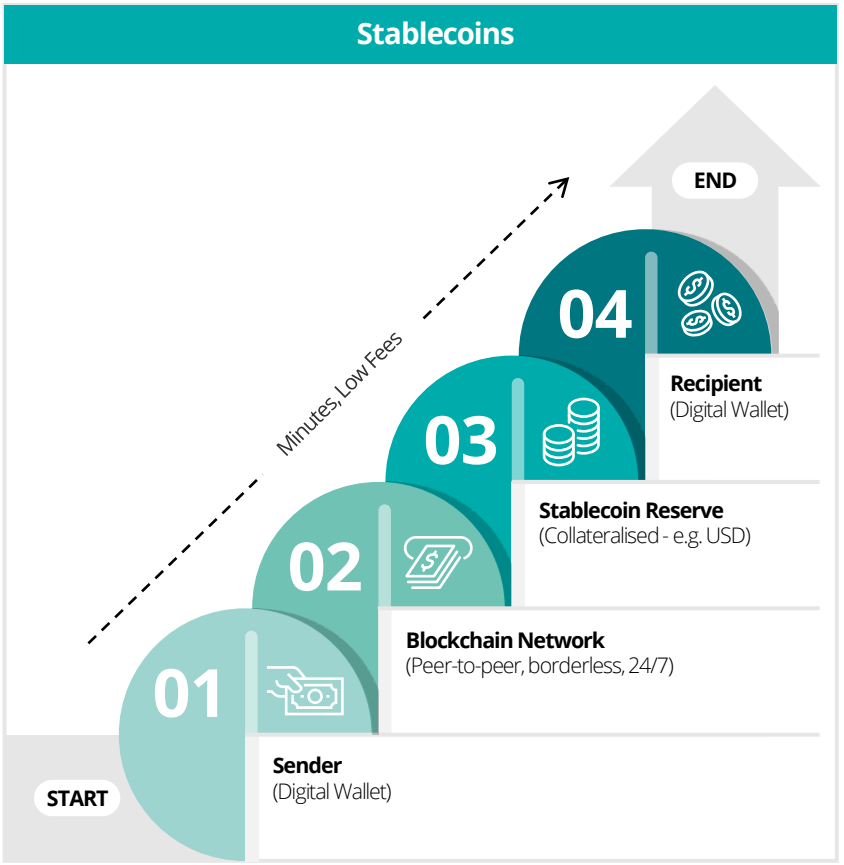


Digital money

Stablecoins

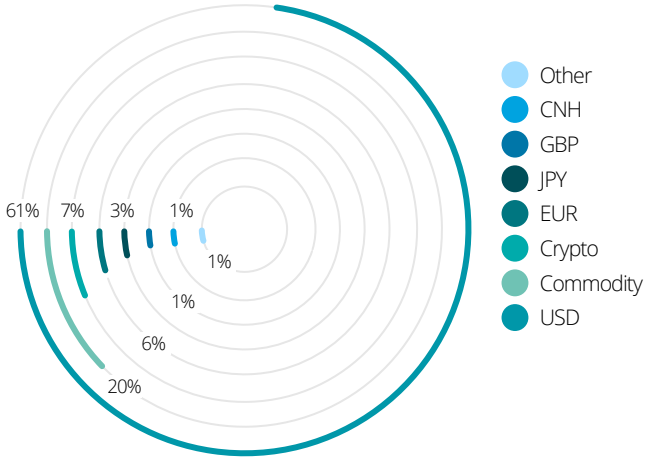
Stablecoins have emerged as a cornerstone of the evolving digital assets ecosystem, with adoption in AP accelerating in line with global trends. By anchoring value to fiat currencies or commodities, they dampen volatility compared to other types of cryptocurrencies. Stablecoins also offer 24/7 instant settlement and lower transaction fees, making them an attractive choice for cross-border payments, remittances, and capital preservation. For example, market participants are using stablecoins as a 'cash-like' settlement asset, instead of relying on bank transfers for settlement. Retail use of stablecoins is also gaining traction; with fewer intermediaries than traditional banking, fees can be lower than card or bank transfers. Further as Web3 and decentralised finance (DeFi) expand, stablecoins are also becoming a foundational aspect of the next generation financial infrastructure.



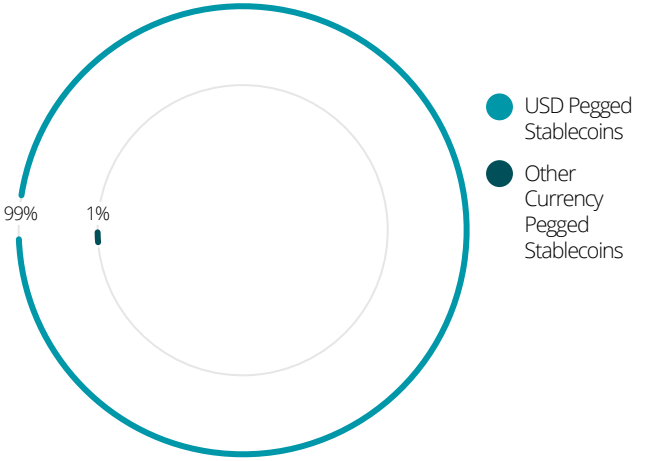


The number of stablecoins in active use globally has surged from roughly 60 in mid-2024 to over 170, and market capitalisation has increased by over 100% in two years to around $255 billion by June 2025.[78] However, the market remains highly concentrated (around 90% of market value is held by two issuers), and overwhelmingly USD-denominated (nearly 99% by market value).

Stablecoin Backing by Quantity (%)



Global Market Capitalisation (%) (Estimate)



*Bank for International Settlements, BIS Bulletin No 108 Stablecoin growth – policy challenges and approaches, July 2025 Stablecoin growth - policy challenges and approaches

Stablecoins do not always remain stable, with some experiencing periods of volatility exceeding that of stocks or other crypto assets. Even fiat-backed coins may trade slightly above or below par on secondary markets. Further, well-known de-peg episodes also highlight liquidity and design risks, calling into question their reliability for everyday payments.

There is also concern around the growing prevalence of stablecoin used in illicit activities. Stablecoins move easily across public, borderless blockchains and into self-custody making know your customer (KYC) controls more difficult to implement effectively.

With the proliferation of stablecoins, regulators throughout the AP region are increasingly focused on crafting robust frameworks which foster innovation, while also safeguarding financial stability, consumer/investor protection and preventing financial crime. Requirements typically focus on minimum levels of capital and reserves, timely redemption, disclosures, and robust rules covering segregation of assets and custody arrangements. With respect to financial crime there is also a focus on ensuring robust rules around KYC and anti money laundering / counter terrorist financing (AML/CTF).

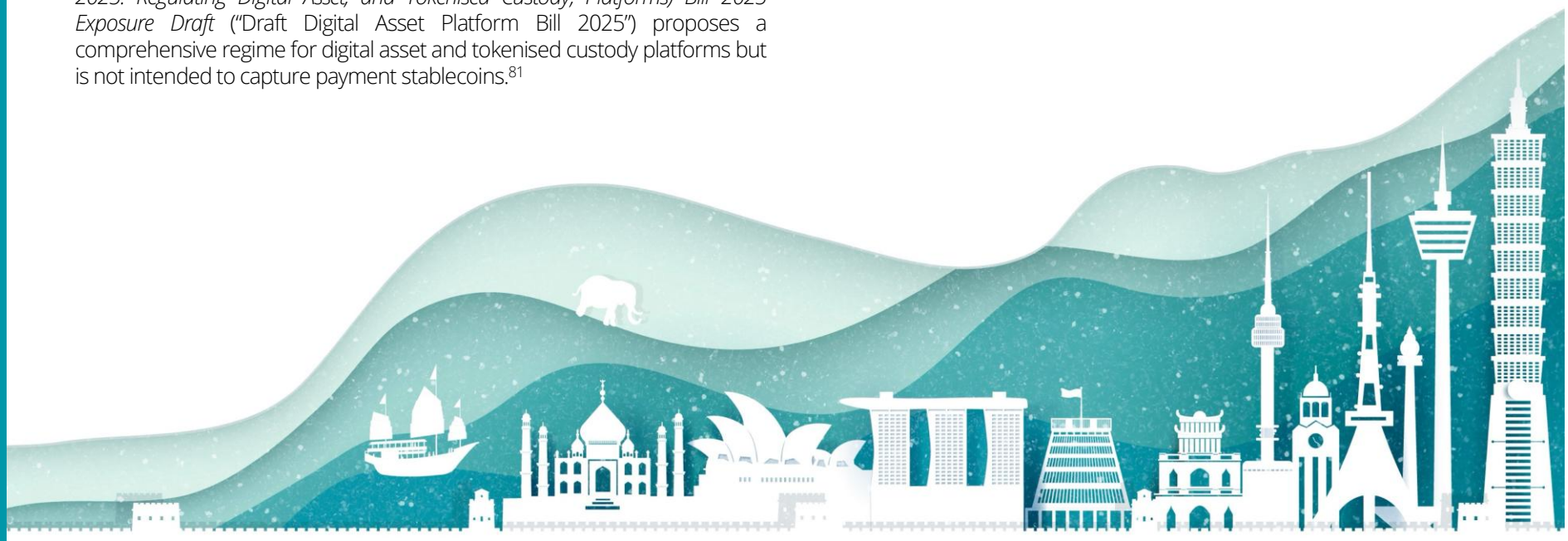
Understanding the region's diverging approaches is increasingly important. China has banned crypto transactions outright and prohibited the use of stablecoins as payment instruments. Stablecoins in some jurisdictions such as Indonesia and India whilst not banned exist in a regulatory grey area under existing digital asset rules. Other regions regulate stablecoin under broader payments or crypto-asset frameworks; with a growing number of jurisdictions now developing or considering stablecoin-specific regimes.

In October 2025, Japan recorded a notable milestone with the issuance of the first yen-pegged stablecoin (JPYC)[79], regulated under Japan's revised *Payment Services Act*[80] (in force since 2023) which treats fiat-pegged "digital money-type" stablecoins as electronic payment instruments which can be issued by licensed banks, fund transfer service providers, and trust bank.

In Australia, the government is introducing the Australian Treasury's draft payments licensing reforms, which would regulate stored value facilities linked to payment stablecoins as financial products—though not necessarily the digital tokens themselves—and establish a new class order for stablecoin intermediaries. Additionally, *the Treasury Laws Amendment Bill 2025: Regulating Digital Asset, and Tokenised Custody, Platforms) Bill 2025 Exposure Draft* ("Draft Digital Asset Platform Bill 2025") proposes a comprehensive regime for digital asset and tokenised custody platforms but is not intended to capture payment stablecoins.[81]

Further, the newly released *Tranche 1a Exposure Draft legislation*[82] ("Exposure Draft") proposes amendments to the *Corporations Act 2001*[83], introducing definitions and regulatory requirements for payment services, including those involving stablecoins, by focusing on the underlying facilities and their providers rather than the tokens themselves. The reforms align with international best practice and are technology-neutral, with further details on exemptions and prudential regulation expected in subsequent legislative tranches.

In September 2025, the ASIC introduced a new class exemption *(ASIC Corporations (Stablecoin Distribution Exemption) Instrument 2025/631)*[84] allowing intermediaries to distribute certain Australian-issued stablecoins without having to apply for a separate Australian Financial Services ("AFS"), license to operate a market, or clearing and settlement facility licences, provided the issuer holds an AFS licence. This targeted exemption serves as an interim measure ahead of the implementation of the full regulatory framework under the Exposure Draft, enabling stablecoin issuers to operate in the meantime.



South Korea's regulatory environment for stablecoins is evolving rapidly. As of June 2025, the *Digital Asset Basic Act*[85] permits Korean firms to issue stablecoins pegged to the South Korean Won, providing a legal foundation for domestic stablecoin issuance and use. In addition, two further draft bills are under consideration, both proposing a more relaxed regulatory approach to stablecoin issuance, potentially reducing compliance burdens and encouraging innovation in the digital asset sector.

Hong Kong has also taken an active approach towards regulating stablecoins through the creation of a licensing regime with bespoke guidance and fiat capital reserve requirements under the *Stablecoins Ordinance*.[86] The licensing regime became effective on 1 August 2025 under the supervision on the HKMA which released an explanatory note on the licensing process[87], as well as guidelines on the supervision of stablecoin issuers[88] and the AML/CTF expectations for these market players.[89] Key requirements include maintaining full backing of stablecoins with high-quality, highly liquid reserve assets, robust governance and risk management frameworks, regular audits, segregation of reserve assets, and clear redemption mechanisms to ensure users can redeem stablecoins at par value. Issuers must also provide transparent disclosures on the stabilisation mechanism, risks, and operational details, and are restricted from engaging in lending or investment activities using reserve assets.

As of 30 September 2025, HKMA received 36 stablecoin license applications from banks, technology firms and other financial institutions.[90] The authorities have signaled that the initial cohort will be announced in early 2026 and is expected to be small in order to support effective supervision.

Conversely, China maintains a restrictive stance on domestic stablecoins, while advancing its central bank digital currency (CBDC), the e-CNY. At the Annual Conference of the Financial Street Forum 2025, People's Bank of China (PBOC) Governor, Pan Gongsheng cited shortcomings in customer identification and AML/CTF compliance as key concerns.[91] This position was reinforced at a November multi-agency meeting convened by the PBOC to curb speculation in virtual-asset trading.[92] During the meeting, officials reiterated that stablecoins lack legal tender status, are barred from use in market transactions, and pose heightened risks including money laundering, fraudulent fundraising, and illicit cross-border transfers.

Debate over the "dollarisation" from the use of stablecoins

One of the key risks associated with the emergence of US dollar backed stablecoins is the concept of "dollarisation" whereby consumers particularly in emerging economies may use such financial instruments in lieu of their local currency.[93] This mirrors the real economy whereby the US Dollar acts as the global reserve currency. There is significant potential for systemic risks to emerge in economies due to the potential for currency instability and devaluation, degradation of the traditional banking system, and the potential for money laundering. On the other hand, US Dollar backed stablecoins could provide significant opportunities and benefits in relation to cross-border transactions outside of the traditional payments framework (and associated costs). In an environment where the role of the United States is changing in the global geopolitical and economic landscape, the proposition of US dollar backed stablecoins is a complex one for jurisdictions across the AP region.

Central bank digital currencies

Central bank digital currencies (CBDCs) are also progressing, with AP emerging as a global leader in exploration and development. As governments and central banks across the region consider and implement CBDC initiatives, regulatory frameworks are evolving to address key challenges such as financial inclusion, security, and cross-border interoperability. The growing debate surrounding CBDCs highlights their potential to transform payment systems and enhance monetary policy tools.

The e-CNY (digital yuan) remains integral to China's financial infrastructure transformation, with the PBoC advancing nationwide adoption through pilot programmes across 26 provinces and major urban centres like Shanghai and Shenzhen. Integration has broadened in retail, transport, and public services via collaborations with commercial banks and technology platforms. Payment volumes of the e-CNY showed a significant increase reaching RMB 14.2 trillion in September 2025, up from RMB 7.3 trillion in July 2024.[94]

Hong Kong has also been conducting an ongoing trial of its CBDC the e-HKD. The HKMA issued the "e-HKD Pilot Programme - Phase 2 Report" in October 2025 which summarised the conclusions of the second phase of the e-HKD pilot program.[95] The second phase focused on the "commercial viability and scalability" of the real-world use cases for the e-HKD. Looking forward, the HKMA will establish the legal and regulatory framework in the first half of 2026 for the retail deployment of the e-HKD as well as supporting the use of the wholesale e-HKD by financial institutions.

India's wholesale CBDC (e₹-W) is fully operational and widely used by major banks for interbank settlements, enhancing efficiency and security in wholesale financial transactions since its 2022 pilot and 2024 adoption. In contrast, the retail CBDC (e₹-R) remains in an extended pilot phase since its 2022 pilot, with millions of users and thousands of merchants participating across numerous cities and select rural areas. While the retail Digital Rupee has seen considerable adoption and supports features such as offline payments and interoperability with existing digital payment systems, it has not yet reached full national rollout.

Conversely, in South Korea, the Bank of Korea (BOK) has stated that it has not decided whether or not to issue a CBDC.[96] However, as discussed above it has been active in pursuing stablecoin issuances, highlighting the variance of preferences and priorities across the region.

In 2026, CBDC pilots are likely to tighten links with banks, expand use in trade settlement, and compete more directly with stablecoins, especially if designs include remunerated balances similar to demand deposits. Policy priorities will focus on privacy, supervisory access, and resilient technology and infrastructure.

China stands out for pace: the e-CNY has moved from trials to broad use faster than most other regions, and a nationwide rollout could arrive as soon as this year. Given its scale and strategic backing, the e-CNY will remain central to China's economy and to global discussions on the future of money.

Tokenised deposits vs stablecoins

Tokenised deposits have also seen a significant increase in regulatory attention as well as adoption by financial services firms. Rather than one replacing the other, both stablecoins and tokenised deposits are likely to serve different purposes within the financial ecosystem.

The approach of financial services to adopting tokenised deposits and stablecoins within their payments infrastructure is dependent upon their strategy, scale, service offering, location, and their willingness to take on risk.

Tokenised deposits provide firms with a practical tool for handling liquidity across international borders and time zones. They also allow firms to accrue interest and simplify the navigation of regulatory and auditing requirements, as well as to settle transactions involving tokenised assets. Alternatively, stablecoins operating on public blockchains are positioned to streamline consumer payments and facilitate international bank to bank (B2B transfers).

Some key regulatory developments in relation to tokenised deposits include:

Jurisdiction	Public-private partnership

Australia
The RBA, ASIC, and the Digital Finance Cooperative Research Centre (DFCRC) announced the launch of Project Acacia, testing how different forms of digital assets and relevant infrastructure can develop the tokenised asset market.[97] The final report of the project is expected in Q1 2026.

Hong Kong
The HKMA announced the launch of Project Ensemble which seeks to enable real-value transactions involving tokenised deposits following a successful sandbox exercise. This looks set to enable participating banks to use tokenised deposit transactions through a real-time settlement system.[98]

Singapore
The MAS has continued to explore the use cases of tokenised assets through Project Guardian. The MAS issued a report focusing on how tokenisation can support transaction banking through the streamlining of FX payments and settlements.[99] Other Project Guardian reports focus on the operationalisation of tokenised money market funds, and the tokenisation of fixed income instruments.[100]

Regulators across AP look set to follow the global trend of exploring use cases for tokenised deposits. 2026 is likely to see continued experimentation with stablecoins and tokenised deposits as regulators and financial services firms seek to optimise efficiency and enhanced settlement latency. While largely still in pilot phase, we see significant potential for scaling tokenized deposits given the size of traditional deposit market across AP.

Looking ahead, there are also signs of growing demand for tokenized instruments beyond deposits, including fund units, money market funds, bonds and securities etc. This is a pattern we expect to continue into this year and beyond.

Overview of key digital money models

The table below summarises the core differences and primary emerging use cases of the key digital money models discussed in this section.

	Stablecoins	Tokenised deposit	CBDC
Issuer	Private entity	Commercial bank	Central bank
Main Infrastructure	Public blockchain networks	Permissioned token platform linked to bank deposit system	Central bank-led platform
Overview	Represents a claim on the issuer and its reserve backing (structure depends on the regime). Designed to keep a stable value (often pegged to a currency like USD)	Represents a bank deposit claim on the issuing bank (a deposit 'in token form')	Represents a direct claim on central bank money (sovereign currency) with specific design often varying for retail vs. wholesale markets
Use Cases	Frequently used for cross-border transfers, and as a 'cash-like' settlement asset	Currently used mainly for institutional settlement (e.g., tokenised securities, repo/collateral), and treasury/ liquidity movement within bank networks	Currently used in pilots for wholesale settlement and/or retail payments
Benefits	Can move value 24/7, often faster than traditional transfers; may reduce friction for certain corridors; supports on-chain activity	Combines the familiarity of deposits with benefits of tokenisation - faster institutional settlement and programmability - while staying within a bank-based framework	Potential for more efficient settlement; can support policy goals (e.g., resilience, central control) depending on design; may improve wholesale settlement in specific use cases
Drawbacks	Reserve quality and redemption under stress; governance and disclosures; AML/CFT effectiveness; operational resilience of issuer and networks	Legal/structural clarity (is it treated as a deposit everywhere); interoperability depends on participating banks/standards; operational resilience and concentration of providers	Design and governance choices (privacy vs traceability; intermediated vs direct); adoption incentives; operational resilience; cross-border interoperability is complex

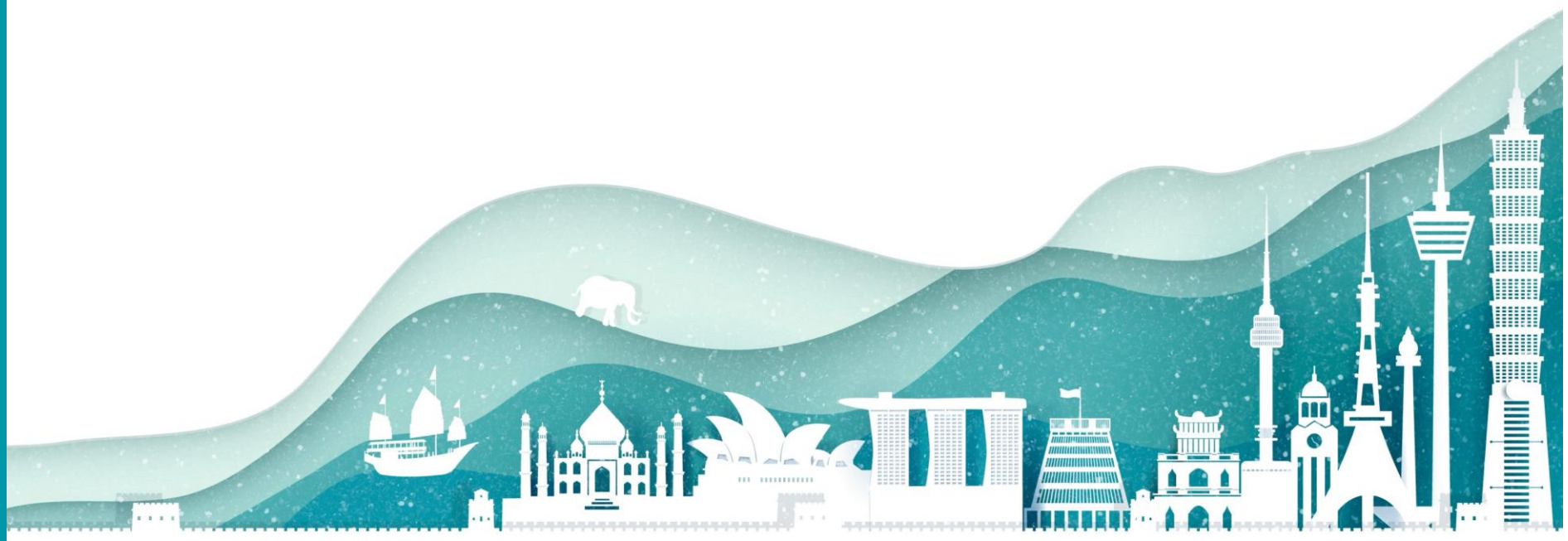
Digital money is beginning to scale, however regulators, financial services firms and customers are increasingly expressing different preferences across stablecoins, tokenised deposits and CBDCs depending on use case and regional priorities. Financial institutions will need to carefully balance these priorities across the jurisdictions they operate in.

The broader regulatory landscape for digital assets

Across AP, regulatory frameworks for digital asset trading platforms, custody and related service providers are evolving rapidly, extending licensing, safeguarding of client assets and cyber/operational controls. Consumer appetite for different forms of digital assets is growing and regulators are updating their rulebooks to ensure consumer protection and promote stable growth.

Australia

Australia has made a significant legislative change in November 2025 to modernise the regulatory regime governing digital assets. The "Corporations Amendment (Digital Assets Framework) Bill 2025" was introduced which brings digital asset and tokenised custody platforms in to the mainstream financial regulatory oversight regime, meaning that the Australian Financial Services (AFS) licensing and consumer protection requirements applied to traditional financial institutions and product offerings are extended to digital assets providers and products.[101] If the proposals are adopted by Parliament, there will be an initial 12 month period before the Bill becomes effective and an additional 18 month transition period for firms to comply with the requirements.[102]



Hong Kong SAR

Hong Kong has maintained its regulatory focus on promoting the use of digital assets in the jurisdiction. The SFC released their regulatory roadmap for Hong Kong's virtual asset market which outlines their five-pillar approach to "future-proof Hong Kong's virtual asset ecosystem" through twelve initiatives designed to promote Hong Kong as the regional hub for digital assets.[103] The SFC introduced a streamlined licensing regime and external assessment process for new virtual asset trading platform (VATP) applicants, effective 18 December 2024.[104] VATPs are required to implement robust systems and controls, and enter a tripartite agreement with an external assessor (EA) and the SFC to ensure regulatory compliance. The SFC has also clarified its expectations for VATP operators, emphasising strong cyber security, privileged access management, secure storage of client assets, and comprehensive contingency plans. Hong Kong expanded the offerings available to VATPs by allowing them to provide staking services, this is the process of participating in the network of a blockchain by locking up a certain amount of coins or tokens to support various operations, such as transaction validation, security, and governance.[105] Further to this, the HKMA announced it would permit authorised institutions to provide staking services from custodial VA services for clients subject to compliance with a bespoke regulatory framework.[106]

Hong Kong has also aligned its capital standards, disclosure and exposure limits with the recommendations of the Basel Committee in relation to cryptoassets. The HKMA released a supervisory policy manual on the 'Classification of Cryptoassets'[107] in accordance with the Basel Committee's standards on the 'Prudential treatment of cryptoasset exposures'[108] and 'Cryptoasset standard amendments'.[109] The Hong Kong government introduced the *Banking (Capital) (Amendment) Rules 2025, Banking (Disclosure) (Amendment) Rules 2025*[110] and the *Banking (Exposure Limits) (Amendment) Rules 2025*[111] to legislate the changes which are effective from January 2026, with the HKMA supervisory manual providing practical guidance.

Looking forward, the key developments in Hong Kong will likely be in relation to the proposed virtual asset custodian licensing regime. The Financial Services and the Treasury Bureau (FSTB) in collaboration with the SFC issued a public consultation proposing a bespoke licensing regime for firms providing virtual asset custodian services.[112] The FSTB and SFC are in the process of reviewing the results of the submission ahead of the introduction of the licensing regime.

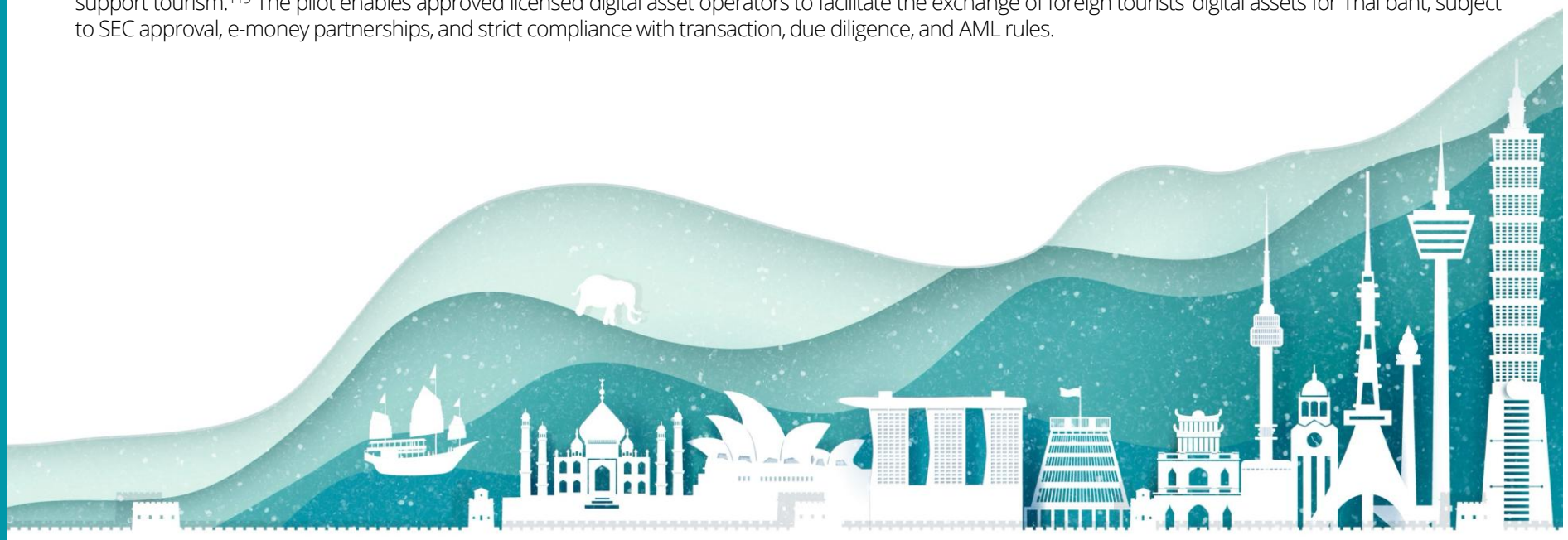
In contrast, China has maintained its official ban on cryptocurrencies and with the PboC announcing a further crackdown on crypto miners in November 2025.[113]

Singapore

Singapore in a similar manner to Hong Kong aligned its cryptoasset exposures for Singapore-incorporated banks in line with the Basel Committee's standards, effective from January 2027.[114] The MAS also finalised the Digital Token Service Providers (DTSP) regulatory regime, with the regulation coming into effect in June 2025.[115] The DTSP regulatory regime applies to Singapore incorporated firms providing digital token services outside of Singapore.

Thailand

Thailand demonstrated an active regulatory focus on digital assets. The Securities and Exchange Commission of Thailand (SEC Thailand) has announced that USD Coin (USDC) and Tether (USDT) are now permitted for transactions by digital token issuers and digital asset operators, joining Bitcoin, Ethereum, Ripple, and Stellar.[116] SEC Thailand also updated exemptions for digital assets fund management, allowing licensed securities companies managing digital assets for mutual or private funds to be exempt under certain conditions.[117] Additionally, new guidelines were issued that clarify that digital asset business operators who fully comply with the Thai Digital Asset Operators Trade Association's protocols for managing mule accounts will be considered complaint with SEC standards.[118] Mule accounts are utilised to move money through a financial system without revealing the owner's identity, mule crypto accounts are increasingly being used by criminals to circumvent the traditional financial system. Further, the SEC Thailand launched an 18-month pilot, TourstDigiPay, to support tourism.[119] The pilot enables approved licensed digital asset operators to facilitate the exchange of foreign tourists' digital assets for Thai baht, subject to SEC approval, e-money partnerships, and strict compliance with transaction, due diligence, and AML rules.



Key trends to watch in 2026

Regulatory harmonisation and standardisation
As Asia Pacific jurisdictions develop divergent frameworks for CBDCs, stablecoins, and digital assets, regulatory fragmentation remains a key challenge. In 2026, regulators will continue to build out their frameworks for governing digital assets. Harmonisation across the region is unlikely in the short term, but increased regional regulatory discourse may steer regulatory trends in the medium to long term. Firms must be proactive in monitoring developments, engaging with regulators, and participating in standard-setting initiatives to both stay ahead of developments and influence the evolving regulatory landscape.

Strengthening operational resilience
Digital asset custody, settlement, and reconciliation present unique operational risks. Regulators are set to introduce more prescriptive requirements for safeguarding client assets, managing key processes, and ensuring business continuity. Firms will need to demonstrate robust controls, clear segregation of duties, independent reconciliations, and resilience in the face of operational incidents. Transparency in reserve management and escalation procedures, especially for CBDCs and stablecoins, will be increasingly scrutinised.

Heightened focus on financial crime and transaction monitoring
The expansion of digital assets heightens the risk of fraud, money laundering, and terrorist financing. In response, regulators will require firms to deploy advanced, technology-enabled AML/CFT controls, such as real-time transaction monitoring, blockchain analytics, and enhanced due diligence for high-risk wallets or jurisdictions. Firms will need to evidence effective governance, and rapid identification of and escalation of suspicious activity.

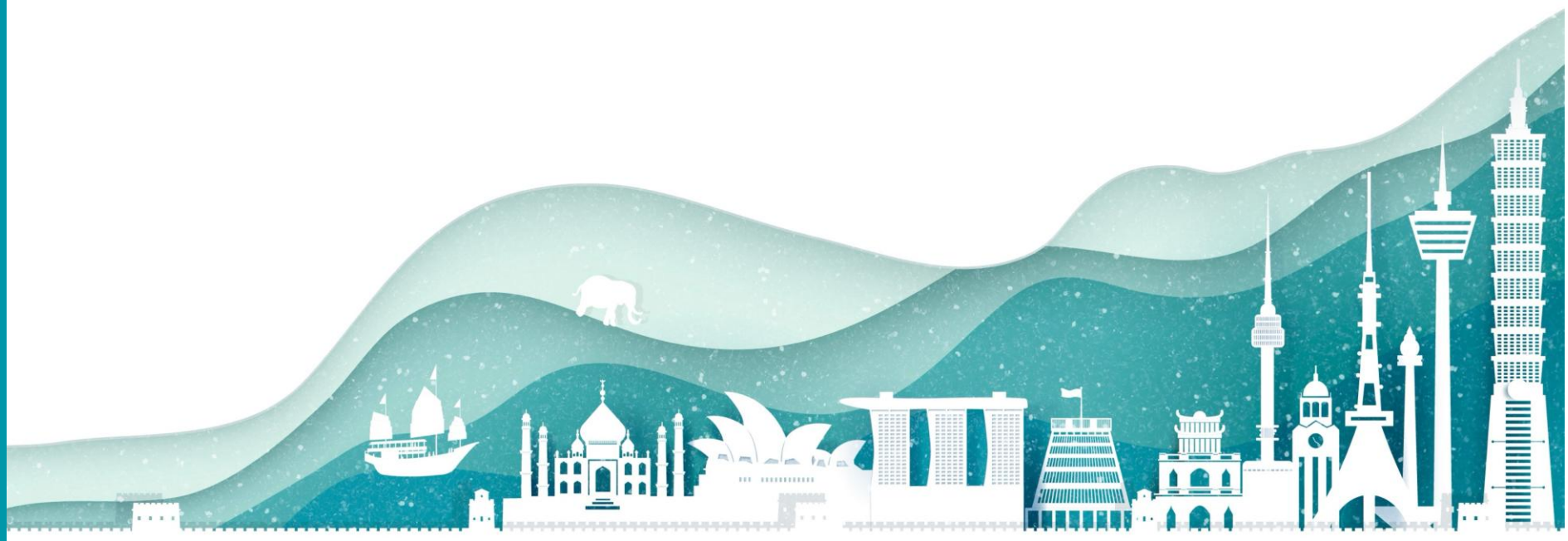
Navigating cross-border complexity and interoperability
Inconsistent regulatory approaches and a lack of interoperable technical standards continue to hinder cross-border digital asset transactions. In 2026, regulators will focus on enabling compliant and efficient cross-border activity through common protocols, data-sharing arrangements, and mutual recognition frameworks. Firms must map their obligations, manage multiple licences, and invest in technologies that support interoperability across platforms and jurisdictions.

Adapting to shifting data and cybersecurity expectations

The digital nature of CBDCs, stablecoins, and other digital assets elevates the importance of strong data protection and cybersecurity. Regulators will introduce more granular requirements for safeguarding sensitive data, managing cyber risks, and responding to incidents. Firms will need advanced security controls, regular cyber risk assessments, and rapid response capabilities. Data localisation and privacy compliance will also remain central to supervisory expectations, particularly for cross-border data flows.

The rapid evolution of digital assets, particularly stablecoins, CBDCs, and cryptocurrencies, is fundamentally reshaping the global financial landscape. As stablecoins gain traction as a medium of exchange and store of value, they present unique risks related to financial stability, consumer protection, and anti-money laundering (AML) compliance. CBDCs, meanwhile, offer significant potential for enhancing payment efficiency and financial inclusion, but they also raise complex questions concerning privacy, monetary policy, and cross-border interoperability.

The regulatory responses to these developments remain fragmented across jurisdictions, reflecting differing priorities and risk appetites. While some regulators have adopted proactive approaches, issuing clear guidance or pursuing bespoke legislative frameworks, others continue to grapple with the pace of technological change and its implications for legacy regulatory structures. Achieving an effective balance will require ongoing dialogue and cooperation among policymakers, industry participants, and international standard-setting bodies.



Financial Crime

Increasing volume, velocity and new attack channels

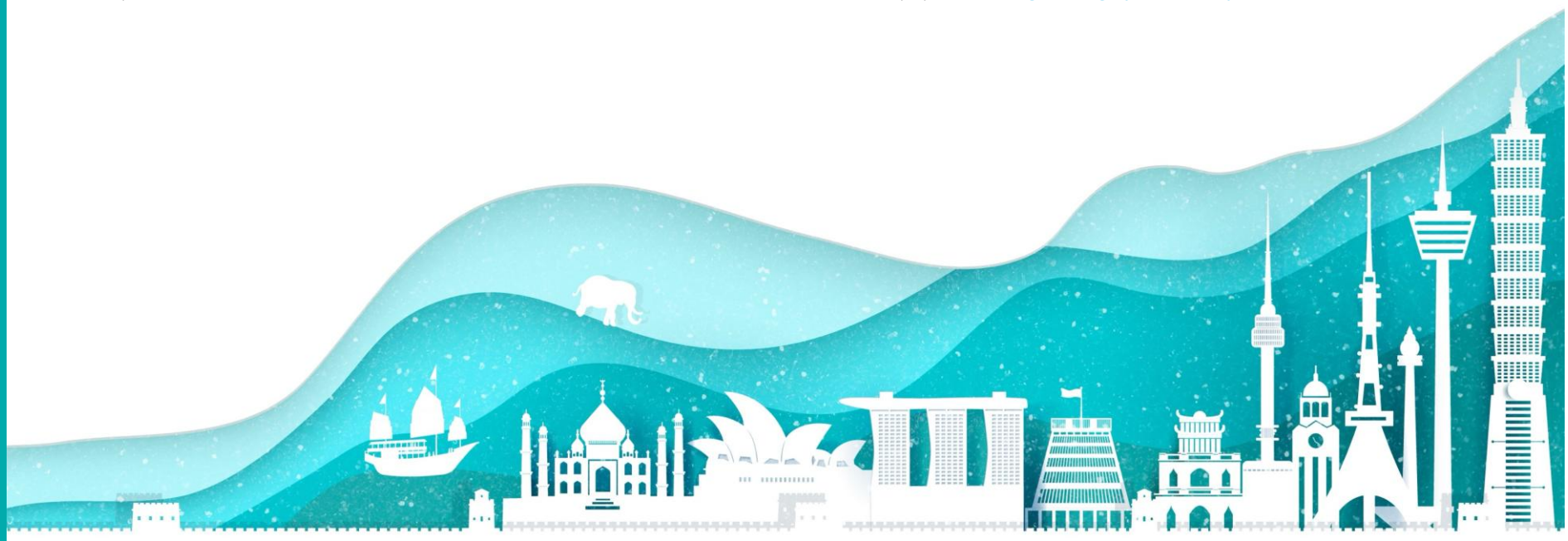
Digital innovation has unlocked new avenues for efficiency and increased revenue for financial services firms. However, it has also created fertile ground for increasingly sophisticated forms of financial crime such as AI and deepfake-related fraud, which was projected to see a 55-60% increase by end-2025.[120]

Malicious actors are harnessing advances in AI to bypass traditional controls, perpetrate fraud, and launder illicit funds at scale. In parallel, the region's embrace of digital platforms and real-time payments has enabled a proliferation of scams that exploit both technological vulnerabilities and gaps in consumer awareness. Regulatory frameworks and industry responses are evolving, but the pace and complexity of these threats demand ongoing vigilance, innovation, and cross-border collaboration.

AI as a driver of financial crime

AI is increasingly being used by bad actors to scale, personalise and conceal financial crime, reducing the cost and skill required to run convincing scams, automate illicit flows, and exploit control gaps. As a result, firms are grappling with higher volume and speed of fraud and money laundering, as well as greater uncertainty over what is "real".

The following diagram highlights how AI is being used to perpetrate financial crime from profiling and impersonation to execution of payments and market manipulation. A detailed overview of AI-enabled attack vectors is also covered in our recent paper on Safeguarding Cybersecurity in AI.



AI-driven escalation of financial crime

START

01

Target & groom

- Automated profiling: scrapes publicly available data (social media, company sites, leaked data) to build a target profile and identify pressure points
- Personalisation at scale: generates tailored outreach by role/sector/location (tone, jargon, language)
- Conversation optimisation: uses sentiment cues to choose the next message that keeps the victim engaged (especially in relationship scams)

02

Impersonate & deceive

- Content generation: produces highly credible phishing, fake "support" chats, and document-style messages (bank formats, internal comms tone)
- Deepfake impersonation: voice cloning and synthetic video to mimic executives/customers and increase trust on calls
- Localisation: real-time translation and cultural nuance to reduce "tells" (grammar, phrasing, idioms) that previously exposed scams

03

Gain access

- Credential capture/ account takeover: moves from engagement to access (e.g. login capture, password reset abuse)
- Verification bypass: prompts victims to approve sign-ins or share one-time codes to complete takeover
- Access expansion: uses the compromised account/ device to reach additional accounts, contacts or systems
- Route switching pivots to alternative accounts/ recovery paths when blocked

04

Execute & move funds

- Real-time payment coaching guides victims through bank process steps (payee set-up, confirmation screens)
- Mule network orchestration recruits/ coordinates mule accounts to receive and complete onward-transfer funds
- Transfer completion strategy optimises amounts/timing and channels to reduce friction at the point of transfer (e.g., split payments, faster rails)

05

Layer & conceal proceeds

- Camouflage: shapes transaction patterns and narratives to look "normal" (timing, amounts, counterparties, descriptions)
- Layering automation moves funds onwards through multi-hop transfers across accounts/ providers/ wallets; adapts routes when blocked
- Evidence shaping can generate supporting "explanations" or documents that appear internally consistent if questioned

06

Influence & disrupt

- Disinformation at scale: bots generate and amplify rumours/"breaking news" to move sentiment (especially in thin markets/digital assets)
- Amplification loops: coordinates posting and engagement to create the illusion of credibility and momentum
- AI-enabled intimidation and disruption (doxxing threats, complaint floods, coordinated harassment) to force rapid payment, supress reporting or overwhelm response channels

- **END**

Illustrative examples:

Fraud & scams (1,2, 4)

- Investment & romance scams
- Customer payment redirection scams
- CEO/ Executive impersonation
- Supplier impersonation (invoice fraud)

Identity & account compromise (2,3)

- Credential theft (phishing / fake login)
- Account takeover
- Fake identity & onboarding fraud (synthetic IDs/ deepfakes)

Laundering & funds movement (4,5)

- Money mule networks & laundering

Market integrity threats (1, 2, 6)

- Market manipulation & misinformation

Staying ahead of adversaries

Firms and regulators must harness advanced AI capabilities not just to match, but to outpace the ingenuity of those seeking to exploit the financial system.

Detection

AI-driven technologies offer firms the ability to detect and prevent financial crime in ways that were previously unfeasible. Machine learning (ML) algorithms can analyse vast and complex data sets in real time, identifying unusual patterns and behaviours that may indicate money laundering, fraud, or market abuse. This includes models designed to learn patterns over time, which can be particularly effective for detecting suspicious transaction sequences. Long Short-Term Memory (LSTM) networks have demonstrated exceptional fraud detection accuracy of up to 94.2%.[121] This is particularly valuable for improving detection across high-volume controls (including transaction monitoring, sanctions detection, name screening, and fraud detection), and for reducing false positives so investigators can focus on the highest-risk cases.

By automating the monitoring of transactions and customer behaviours, AI enables financial institutions to respond to threats with greater speed and accuracy, reducing reliance on manual processes that are often slow and prone to human error. As criminal methodologies and delivery channels evolve rapidly, firms are increasingly focused on shortening "time-to-detect" and "time-to-intervene", and on continuously recalibrating controls to reflect emerging typologies and new payment and distribution rails. This also places a premium on intelligence-led prioritisation by directing investigator effort to the highest-risk cases, rather than diluting capacity across high alert volumes and low-value exceptions. In parallel, firms are using analytics to build more dynamic customer risk models which incorporate a broader set of behavioural (including transaction-based) factors.

Investigation

Moreover, AI can enhance the effectiveness KYC and AML/CTF procedures, which are critical components of financial regulatory regimes in the region. Natural language processing (NLP) and advanced analytics can sift through unstructured data, such as news articles and social media, to identify emerging risks related to clients or counterparties.

This not only strengthens due diligence processes but also helps firms anticipate and mitigate potential threats before they materialise. In parallel, leading institutions are applying "copilot" capabilities to streamline investigation workflows, supporting triage, compiling evidence packs, and drafting consistent case rationales and regulatory reports. This helps to improve consistency and reduce cycle times while maintaining appropriate oversight.

Further, GenAI can accelerate document-heavy work such as extracting and summarising information from onboarding files, periodic reviews and adverse media. It can also support more consistent first-draft narratives for alerts and suspicious activity reporting.

Autonomous execution

Firms are beginning to explore and build-out "agentic AI" approaches, where AI systems can plan and execute multi-step tasks within defined guardrails. In financial crime, this could enable more end-to-end automation across onboarding and KYC refreshes, transaction monitoring, and sanctions or fraud investigations. It could support alert triage and case pack assembly, while maintaining human oversight for material decisions.

Key challenges in financial crime prevention and response

Real-time, cross-channel threats
Criminals exploit multiple channels and jurisdictions faster than traditional controls can respond

Alert volume, false positives and capacity strain
High alert volumes dilute focus, slow investigations and raise costs

Data quality and integration constraints
Inconsistent data across systems limits detection accuracy and increases manual remediation effort

High-cost base and low automation
Manual, case-by-case processes and limited straight-through handling drive high operational costs and constrain scalability as volumes rise

Fragmented controls and operating silos
Fraud, AML, cyber and sanctions processes often operate separately, creating gaps and duplication

Rapidly evolving typologies and new rails
Threats adapt quickly across instant payments, platforms and digital assets, requiring frequent recalibration

Identity complexity and synthetic identities
Synthetic identities and impersonation techniques reduce confidence in onboarding and ongoing customer assurance

Reporting burden and customer friction
Investigators spend significant time producing case memos and onboarding/review remains slow and inconvenient for customers

As GenAI matures, leading banks are moving beyond isolated automation toward "embedded" agentic workflows. This requires clear roles, controlled escalation, and human oversight for material decisions supported by quality assurance and an auditable record of actions and rationale.

GenAI-assisted KYC and lifecycle risk
Evidence synthesis; trigger-based refresh

Identity and impersonation defence
Synthetic identity and deepfake risk signals

Precision monitoring and alert triage
Reduce false positives; prioritise highest-risk cases

Cross-domain control orchestration
Unifies fraud, AML and sanctions signals, typologies & workflows

Investigation copilot and case building
Evidence packs; consistent rationales

Automated reporting
Suspicious transaction and activity report drafting with traceability

Network analytics and early warning
Graph analytics and GenAI to uncover hidden links and patterns

Agentic response playbooks (guardrailed)
Pre-defined and controlled workflows that orchestrate investigation steps

AI and agentic capabilities to address key challenges

Regulatory developments & supervisory priorities

Money laundering & terrorist financing

Strengthening AML/CFT controls remains a core regulatory and supervisory priority. As outlined in our digital assets chapter, a significant number of developments target this sector, reflecting the heightened financial crime risks posed. Regulators across AP are also continuing to update their AML/CTF frameworks and regulatory regimes to keep pace with technological developments and evolving social behaviours.

Australia

Australia has materially modernised and broadened its AML/CTF regime, extending obligations beyond traditional financial institutions to a wider set of "Tranche 2" gatekeeper professions (including lawyers, accountants, real estate agents, and high-value dealers).[122] The new requirements introduce more prescriptive CDD obligations which are tailored to different customer types (sole trader, corporates, trusts etc.) and new rules on beneficial owners and senior managers. The amendments also strengthen governance and oversight including the role of the Board and senior executives, and require that sender and recipient information accompanies every transfer, across both traditional payments and virtual assets. Existing in-scope financial entities and newly regulated VASPs are required to comply with the new rules by 31 March 2026, new Tranche 2 entities must be compliant by 1 July 2026.

Mainland China

A revised national AML Law came into effect on 1 January 2025.[123] This update aims to enhance the legal AML/CTF framework in line with international standards ahead of a Financial Action Task Force (FATF) mutual evaluation scheduled from June 2026 to February 2027.[124]

Japan

The JFSA published a discussion paper on their expectations for financial institutions when validating the effectiveness of their AML/CTF frameworks.[125] The discussion paper also sets out the JFSA's approach to communicating with financial institutions on ML/TF risks and the establishment of monitoring frameworks.

Singapore

Singapore advanced its framework with a new national strategy and a pioneering information-sharing platform. The MAS published its National Anti-Money Laundering Strategy at the end of 2024, outlining a proactive, risk-based approach.[126] The MAS also continued to develop the 'COSMIC' secure platform for financial institutions to share information on customers with suspicious red flags.[127]

Beyond policy, supervisors are sharpening their focus on how AML/CTF controls perform in practice, with closer scrutiny of governance, accountability and the information used to evidence effectiveness. Supervisors want reassurance that firms understand how criminals are using AI and that defences are keeping pace. Further, heightened geopolitical risk will continue to drive an emphasis on sanctions compliance and cross-border exposures, with consistent controls expected across distribution channels and jurisdictions.

Scams

Scams have become a defining feature of the financial crime landscape in the AP region, evolving in scale, sophistication, and impact. Fuelled by the widespread adoption of digital banking, mobile payments, and online investment platforms, scammers are deploying increasingly inventive tactics to exploit individuals and institutions alike. From romance and investment scams to impersonation frauds and phishing attacks, these schemes are causing substantial financial and reputational harm across both emerging and established markets.

The cross-border nature of many scams, combined with the speed and anonymity afforded by digital channels, presents significant challenges for detection, prevention, and enforcement. Criminals have been quick to adapt, leveraging new technologies and social engineering techniques to evade controls and target vulnerable segments of the population. Notably, the surge in scams linked to digital assets and unregulated platforms has further complicated the risk landscape.

Regulators and financial institutions throughout the AP region are under mounting pressure to respond, with a growing emphasis on public awareness, real-time transaction monitoring, and cross-jurisdictional collaboration. As scams continue to proliferate and evolve, robust regulatory frameworks and industry cooperation will be critical to protecting consumers and maintaining trust in the region's financial system.

In May 2025, the International Organization of Securities Commissions (IOSCO) issued a global call to action to combat online financial scams, highlighting the role of platform providers.[128] Regulators across the AP region have been active in releasing guidance or updating regulatory provisions relating to scams and the online platform providers that enable such activities. Some of the key regulatory developments across the region include:

Australia
ASIC expanded its financial scam enforcement capabilities to include social media advertisements as part of its capabilities to remove misleading financial information online.[129]

Hong Kong
The SFC urged online platform providers to monitor alerts published on their website and the IOSCO International Securities and Commodities Alerts Network (I-SCAN).[130]

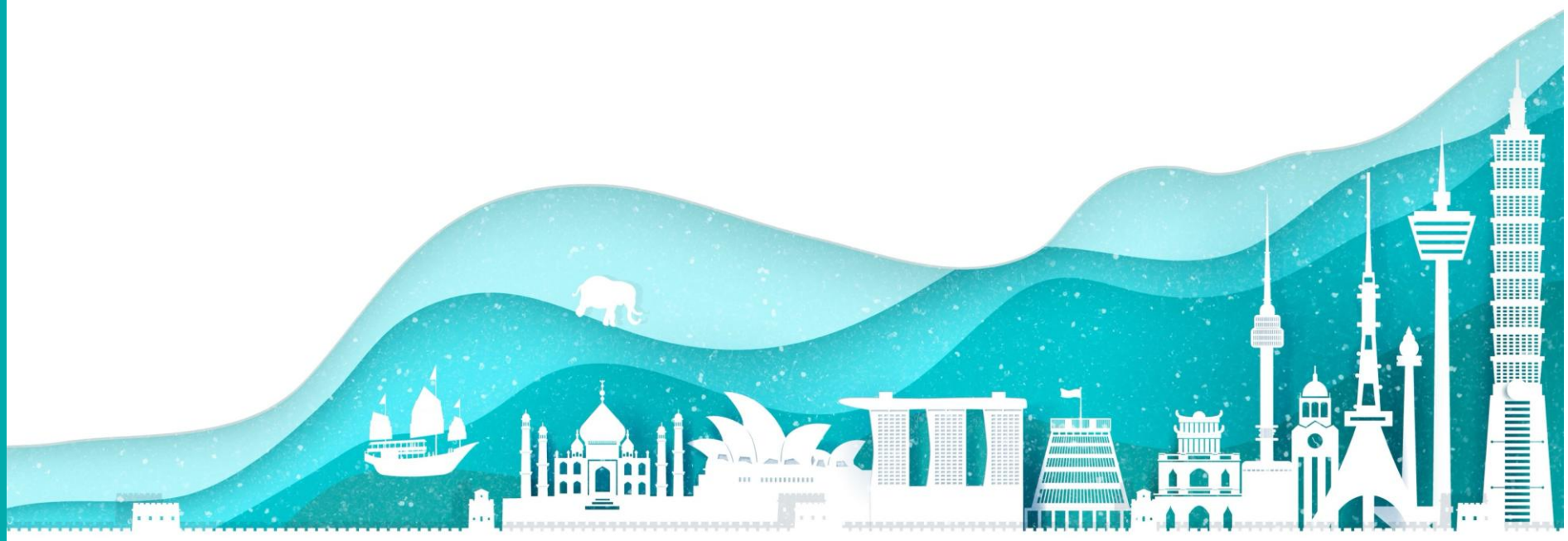
India
The Securities and Exchange Board of India (SEBI) called for greater collaboration in counteracting online scams from social media platforms.[131]

Indonesia
The Indonesian Financial Services Authority (OJK) and the Indonesia Government launched a national campaign to combat financial scams, particularly the emergence of digital scams, through public awareness and enhanced oversight.[132]

South Korea
The Financial Services Commission (FSC) launched an AI-based Anti-phishing Sharing and Analysis Platform (ASAP) to enhance protections against online scams.[133]

Singapore
MAS, in collaboration with the Singapore Police Force and government departments, announced measures to restrict financial criminals from the use of money mules to move money extracted through phone and social media scams.[134]

Online and digitally enabled scams are therefore a key priority for financial regulators across the AP region. Scam volumes are rising as criminals adopt more sophisticated and technology-enabled methods and consumers face greater exposure through social media and other digital platforms. As a result, scams are expected to remain a growing focus for regulators in 2026 and beyond.



Public-private partnerships

A significant development in regulators' campaigns against financial crime is the evolution of Public-Private Partnerships (PPPs) between financial regulatory bodies and industry participants. By fostering collaboration and information sharing, PPPs have the potential to bridge gaps in knowledge, resources, and technological capabilities, enabling more effective detection and prevention of money laundering, terrorist financing, and fraud.

Regulators gain valuable insights into emerging threats and industry practices, while financial institutions benefit from clearer regulatory guidance and access to intelligence that enhances their internal risk management frameworks and financial crime controls. PPPs between financial regulators and industry participants have the potential to create a more resilient and secure financial environment in the face of evolving criminal tactics.

Some examples of PPPs between financial regulatory bodies, government agencies, and industry participants focused on financial crime are:

Jurisdiction	Public-private partnership
Australia	**Fintel Alliance.**[135] Partnership between government agencies, law enforcement, and industry participants to share intelligence and create solutions to detect financial crime.
Hong Kong SAR	**Fraud and Money Laundering Intelligence Taskforce (FMLIT).**[136] A taskforce involving law enforcement, financial regulators and banks to enhance the detection and prevention of financial crime and ML threats.
Singapore	**AML/CFT Industry Partnership (ACIP).**[137] Collaboration between financial sector, law enforcement, and financial regulators to identify emerging AML/CTF risks for Singapore.

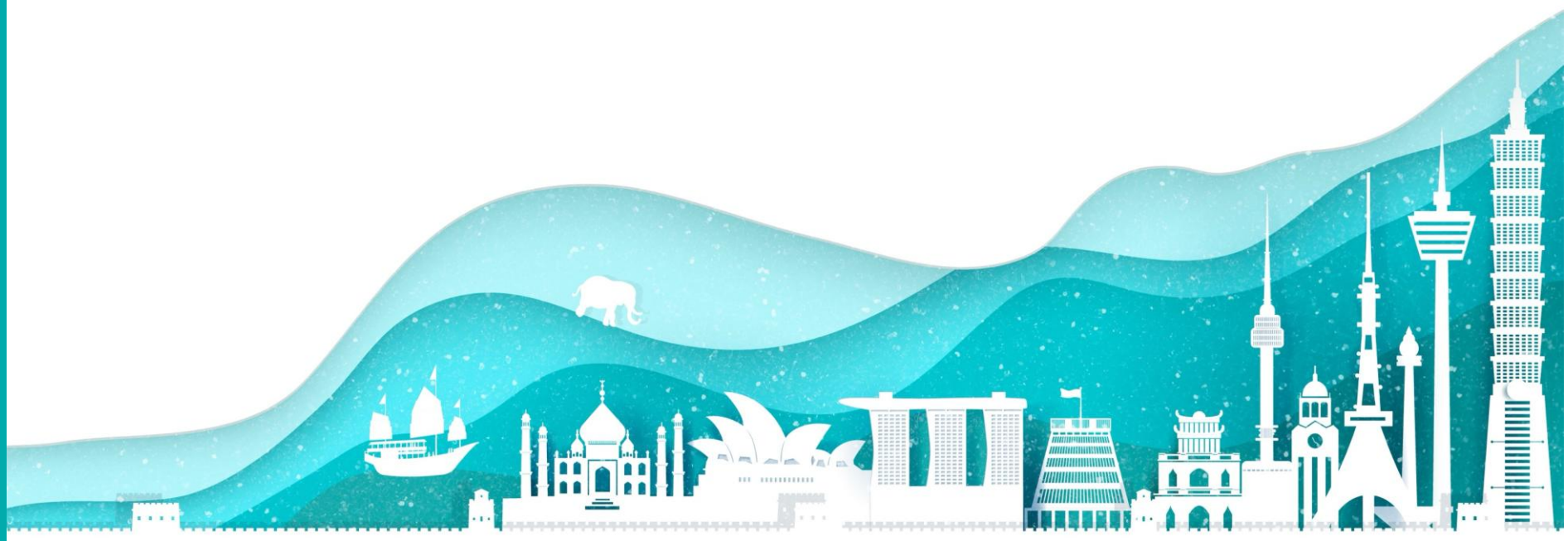
PPPs have become a growing component in Asia Pacific financial crime ecosystem, particularly as criminal operations grow more sophisticated, agile, and global in scope. The increasing prevalence of technology-enabled scams and money laundering schemes, many of which rapidly cross borders and exploit regulatory gaps, has highlighted the limitations of firm-level and jurisdiction-specific responses.

In the AP region there are some examples of formalised collaboration between financial institutions, regulators, and law enforcement agencies that enable the sharing of intelligence, typologies, and best practices. However, existing cross-border mechanisms remain fragmented, and the global nature of organised crime underscores the need for stronger, more coordinated international frameworks. Strengthening cross-jurisdictional PPPs, including through shared data platforms, regional anti-scam alliances, and harmonised response protocols, will be critical to improving detection, disruption, and prevention of financial crime.

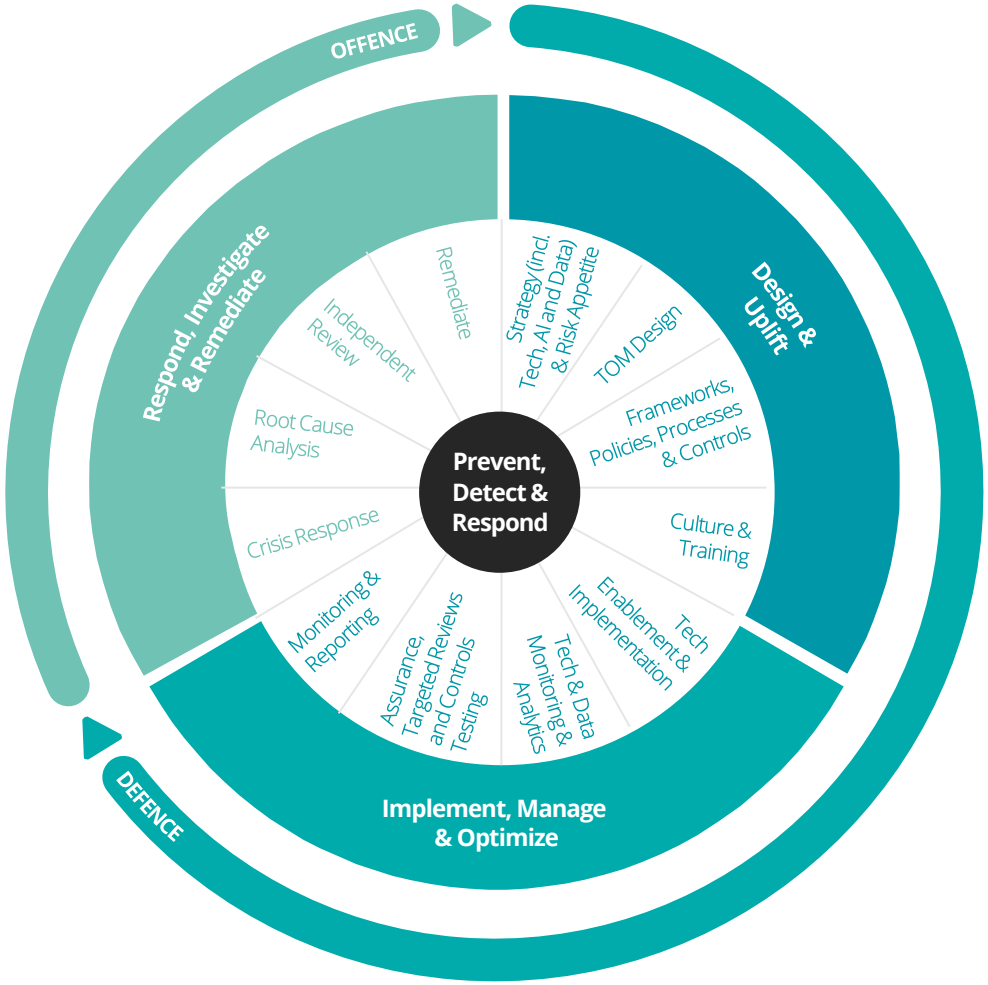
Embedding end-to-end controls across the lifecycle

Financial crime threats are increasingly fast-moving, cross-channel and adaptive, exposing the limitations of fragmented, point-in-time controls. To keep pace, leading firms are shifting from isolated "use cases" toward embedding end-to-end controls across the full lifecycle. This means linking prevention, detection and response in a single operating model. As illustrated in the accompanying diagram, this requires tighter alignment between design and uplift, implementation and optimisation, and response and remediation, so that risk insights and decisions carry through the control chain.

In practice, leading firms are strengthening their ability to prioritise risks dynamically, adjusting due diligence and monitoring as customer and transaction behaviour changes, and reducing manual effort so investigators can focus on higher-risk cases. This depends on integrated data and monitoring across financial crime domains and a feedback loop from investigations and remediation into control improvements.



Financial crime controls across the lifecyle



Leading approaches typically combine six mutually reinforcing capabilities:

01 **Intelligence-led, risk-based control management**
Continuously tuning controls toward the highest-priority risks and emerging typologies, reducing effort where risk is lower

02 **Dynamic customer lifecycle management**
Moving from periodic refresh to trigger-based and continuous due diligence, with automated investigation support where risk changes after onboarding

03 **Modernised operations**
Automating data gathering, consolidation and scoring so smaller, higher-skilled teams can focus on judgement-led disruption and complex networks

04 **Integrated data and technology infrastructure**
Enables better internal and external data sharing and leverages AI/ML to identify complex patterns, improving effectiveness and efficiency

05 **Converged monitoring capabilities**
Integrating indicators across fraud, AML, cyber and sanctions to improve prioritisation, reduce fragmentation and focus investigator capacity on the cases that matter

06 **Proactive public–private collaboration**
Strengthening intelligence sharing and coordinated response with relevant agencies and industry partners to improve detection, disruption and prevention outcomes

Faster Detection → **Better Prioritisation** → **Stronger Disruption**

Key trends to watch in 2026

Escalation and sophistication of tech-enabled scams

The digital transformation of financial services in AP has enabled a surge in the number, variety, and sophistication of scams. Criminals are increasingly using AI to automate attacks, create deepfake identities, and adapt tactics in real time across multiple languages and platforms. Scams are being orchestrated through social media, instant messaging, and real-time payments, often exploiting gaps in authentication and third-party controls. Firms must invest in advanced, adaptive defences and prioritise rapid detection and intervention mechanisms to keep pace.

Rising cost and complexity of compliance

The cost of financial crime compliance is escalating sharply, driven by the need for advanced technology, frequent regulatory updates, and the growing complexity of threats. Firms must continually invest in AI-driven monitoring, skilled personnel, and robust consumer education programmes. Regulators are increasingly expecting technological deployments within institutions' products and services, increasing the cost of compliance. Divergent regulations and fragmented reporting requirements across the region add to the compliance burden, as do increasing expectations for explainability and transparency in AI-based systems. Boards and executives will face mounting pressure to balance risk, cost, and innovation.

Evolving public-private partnerships and regional collaboration

Traditional firm-level responses are no longer sufficient to address new forms of tech-enabled financial crime. Regulators across AP are promoting more formalised PPPs, cross-border information sharing, and intelligence-led initiatives. In 2026, we expect to see enhanced cooperation between the private and public sectors, and growing regional collaboration to combat financial crime. Firms will need to actively participate in these partnerships and adapt their internal processes to leverage shared intelligence while ensuring data privacy and compliance.

Next generation detection and response technologies

The rapid evolution of AI-enabled financial crime requires firms to deploy enhanced detection and response tools. This includes AI-powered transaction monitoring, behavioural analytics, and real-time interdiction systems capable of identifying novel attack patterns and mimicking legitimate customer behaviour. Regulators will expect firms to demonstrate not only technical capability, but also explainability, fairness, and data quality in their AI models. Investment in continuous improvement and the integration of emerging technologies will be critical.

Preparing for the quantum threat

As discussed in our chapter on Artificial Intelligence & Technology, quantum computing is on the horizon and poses a potential paradigm shift in the security landscape. While still nascent, quantum technology could eventually render current cryptographic defences obsolete, making financial systems vulnerable to data breaches and fraud at unprecedented scale. 2026 will see regulators and firms begin to assess quantum resilience, evaluating systems for quantum-safe cryptography and planning long-term transitions. In order to stay ahead of bad actors, it is critical for industry, academics and authorities to come together to future-proof their controls and mitigate these emerging threats.

AI-enabled financial crime and technology-driven scams represent a significant and growing threat to the integrity of the financial system across the AP region. As criminals continue to evolve their methods, financial services firms must not only keep pace with technological advancements but also anticipate the next wave of risks. This requires a holistic approach, combining advanced analytics, robust internal controls, continuous staff training, and strong customer awareness initiatives.

Regulators across the region are intensifying their focus on both AI-related vulnerabilities and the proliferation of scams, yet the fragmented nature of oversight and differing national standards remain barriers to truly effective risk mitigation. Industry-wide cooperation and information sharing will be essential in the fight against cross-border financial crime. Firms must also ensure that their adoption of AI and digital technologies is underpinned by sound governance, explainability, and resilience to emerging threats.

Ultimately, safeguarding the financial system will depend on the ability of firms and regulators to adapt rapidly, foster innovation responsibly, and maintain the trust of consumers and markets. Proactive investment in detection, prevention, and cross-jurisdictional collaboration will be fundamental in meeting the financial crime challenges of 2026 and beyond.

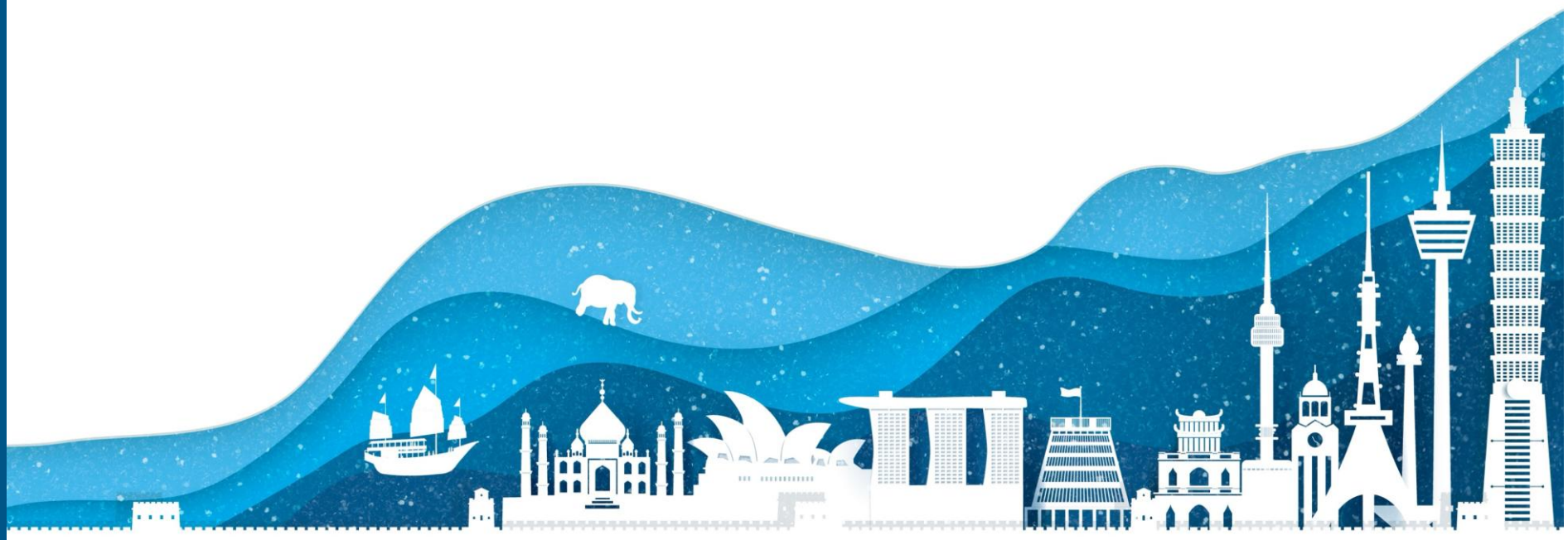
Looking Ahead

As we enter 2026, supervisors will focus on whether strategy, governance and controls are keeping pace with change, and whether firms can evidence consistent outcomes across markets and business lines.

Two cross-cutting forces are reshaping the agenda. Geopolitical fragmentation is increasing uncertainty around trade, sanctions, tariffs and localisation. For financial services firms, this is translating into more complex cross-border operating models, higher friction in client servicing and payment flows and heightened exposure to sanctions compliance risks. At the same time, rapid technological change is accelerating the digitisation of financial services and raising the operational bar for risk management. Together, these drivers are expanding the risk perimeter through more complex supply chains, greater reliance on critical vendors, and faster-moving channels for fraud, market abuse and illicit finance.

Operational resilience is a common thread across these themes. Supervisors will increasingly test whether critical services can be maintained through disruption, including third-party outages, technology incidents, and cyber-attacks. That places renewed emphasis on service mapping, credible contingency arrangements, and the management of concentration and systemic dependencies, including on cloud infrastructure and AI platforms or model providers.

In this environment, risk appetite will take on an increasingly central role and the board and senior management will need to take clear ownership of how it is defined, cascaded, and enforced across the firm. A holistic view of interconnected risks across business lines, markets, and third parties is essential to sustain customer trust and prevent vulnerabilities from scaling into systemic impacts. Even as leaders double down on disruptive technology and operational resilience, prudential fundamentals cannot be allowed to slip. Macro and geopolitical volatility remains elevated and credit quality and liquidity could deteriorate quickly. Therefore, firms must maintain strong financial resilience and credible, tested contingency plans ready to protect capital and liquidity.



Contacts

Authors

Nicola Sergeant
Managing Director
ACRS Operations Lead
Japan
nicola.sergeant@tohmatsu.co.jp

Rhys Belcher
Senior Consultant
ACRS & Hong Kong RFR
Hong Kong SAR
jobelcher@deloitte.com.hk

Asia Pacific Centre for Regulatory Strategy (ACRS)

Nai Seng Wong
Executive Sponsor & SEA Co-lead
Partner
SEA Regulatory Strategy Lead
nawong@deloitte.com

Yuki Shuto
ACRS Steering Committee
Partner
AP Consulting Growth Leader
yshuto@tohmatsu.co.jp

Tony Wood
ACRS Steering Committee
Partner
AP Banking & Capital Markets Leader
tonywood@deloitte.com.hk

Ye Fang
ACRS Steering Committee
Partner
China SR&T FS Industry Lead
yefang@deloitte.com.cn

Sean Moore
Australia Co-lead
Partner
Australia SR&T FS Industry Lead
semoore@deloitte.com.au

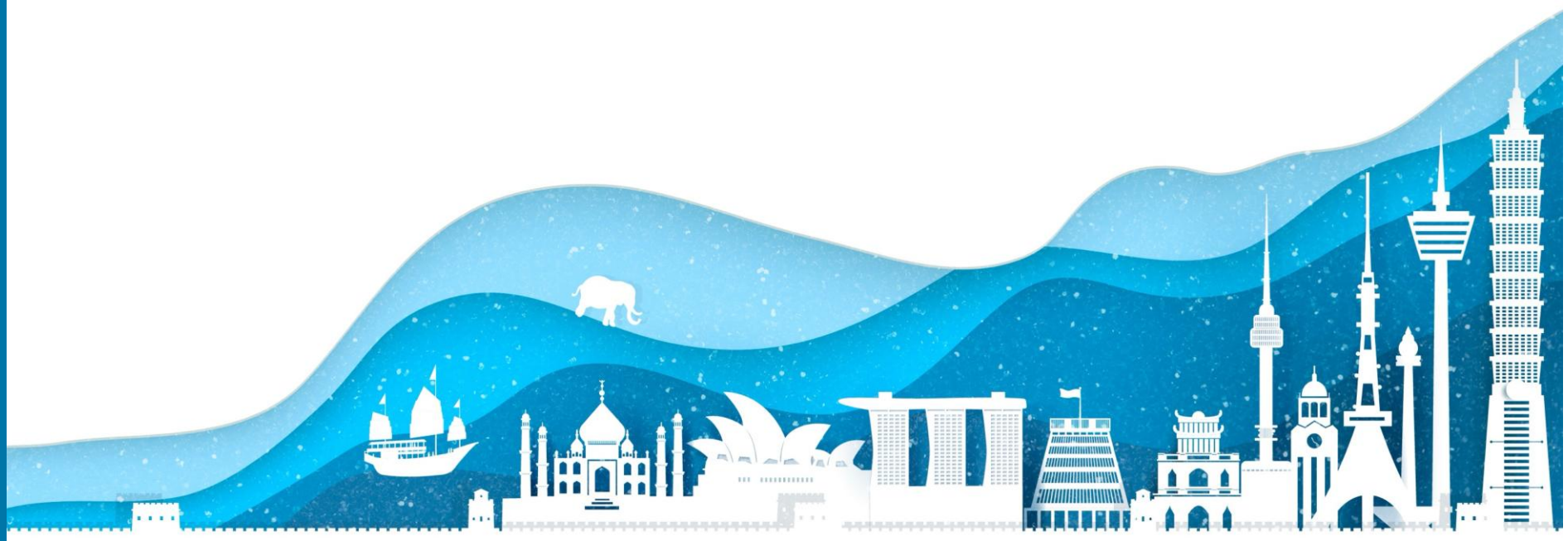
Shinya Kobayashi
Japan Co-lead
Managing Director
Japan SR&T Insurance Sector Lead
shinya.kobayashi@tohmatsu.co.jp

Contributors

Dr Elea Wurth
Partner
Asia Pacific Trustworthy AI Leader
ewurth@deloitte.com.au

Chris Noble
Partner
Asia Pacific Forensic & Financial Crime Offering Leader
cnoble@deloitte.com.au

David Rumbens
Partner
Deloitte Access Economics
drumbens@deloitte.com.au



Endnotes

1. Investopedia, *Big Bang: Meaning, History, Consequences*, June 2023, https://www.investopedia.com/terms/b/bigbang.asp

2. HM Treasury, *Leeds Reforms to rewire financial system, boost investment and create skilled jobs across UK*, July 2025, https://www.gov.uk/government/news/leeds-reforms-to-rewire-financial-system-boost-investment-and-create-skilled-jobs-across-uk

3. HM Treasury, *Financial Services Growth and Competitiveness Strategy: Overview*, July 2025, https://www.gov.uk/government/calls-for-evidence/financial-services-growth-and-competitiveness-strategy/outcome/financial-services-growth-and-competitiveness-strategy-overview

4. US Congress, *"S.1582 - GENIUS Act," 119th Cong.*, July 2025, S.1582 - GENIUS Act. See also Department of the Treasury, *"GENIUS Act Implementation," Federal Register*, September 2025, GENIUS Act Implementation. The Agencies will be required to issue final regulations by July 2026

5. California Senate Bill 53 (2025–2026), *"Artificial intelligence models: large developers"*, September 2025, Bill Text: CA SB53 | 2025-2026 | Regular Session | Chaptered | LegiScan; New York Department of Financial Services, *"Updated Guidance on Custodial Structures for Customer Protection in the Event of Insolvency"*, September 2025, Industry Letter - September 30, 2025: Updated Guidance on Custodial Structures for Customer Protection in the Event of Insolvency | Department of Financial Services

6. Previously known as the Capital Markets Union, the Savings and Investment Union is a package of legislative initiatives aimed at developing integrated capital markets in the EU and channelling household savings into investments

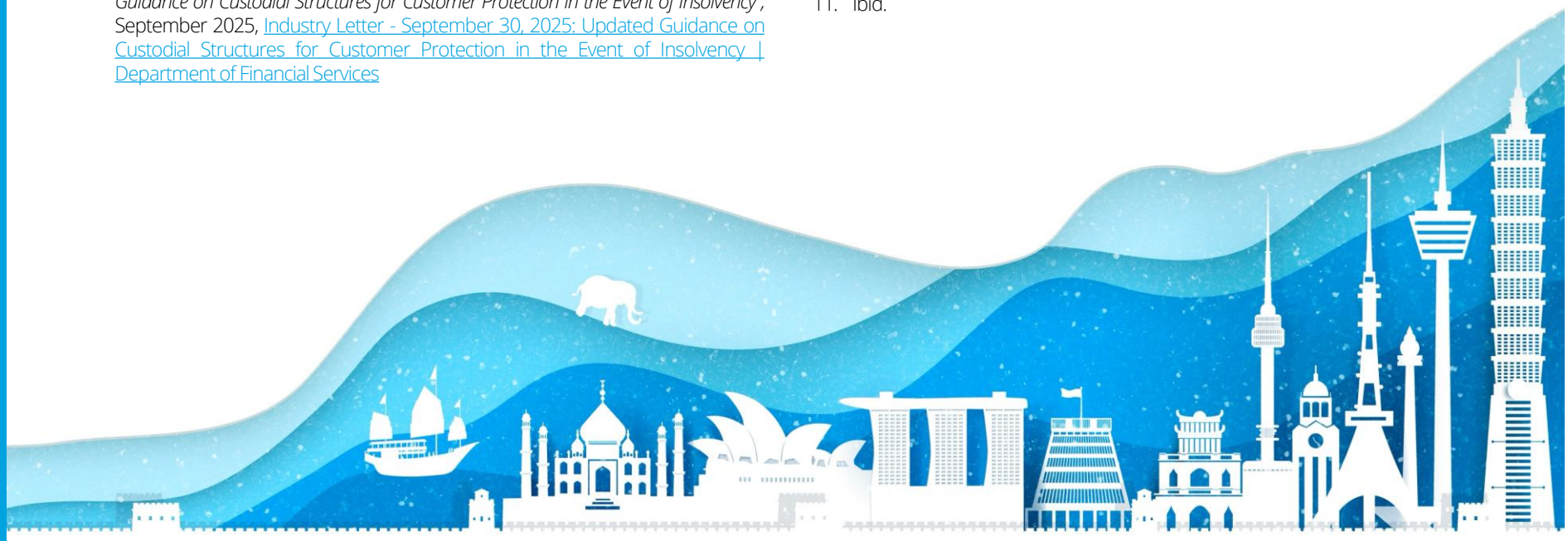
7. The Retail Investment Strategy is a package of measures introduced in 2023 to improve transparency, standardisation, and accessibility of investment products and services for retail investors in the EU

8. The UK Financial Conduct Authority (FCA) proposed "Targeted Support" as a new service that firms could offer. This aims to help many consumers with pension and investment decisions by bridging the gap between general information and personalised advice. It does this by providing group-based suggestions from limited data, with firms needing to clarify that it is not personalised advice.

9. FCA, *CP25/27: Motor finance consumer redress scheme*, October 2025, https://www.fca.org.uk/publications/consultation-papers/cp25-27-motor-finance-consumer-redress-scheme

10. BIS, *The global drivers of private credit*, March 2025, https://www.bis.org/publ/qtrpdf/r_qt2503b.htm

11. Ibid.



12. Federal Reserve Bank of Boston, *Could the Growth of Private Credit Pose a Risk to Financial System Stability?*, May 2025, https://www.bostonfed.org/publications/current-policy-perspectives/2025/could-the-growth-of-private-credit-pose-a-risk-to-financial-system-stability.aspx

13. Reuters, *Private markets brace for cycle test, Asia exits remain tight*, October 2025, https://www.reuters.com/world/asia-pacific/private-markets-brace-cycle-test-asia-exits-remain-tight-2025-10-02/

14. ECB, *Hidden leverage and blind spots: addressing banks' exposures to private market funds*, June 2025, https://www.bankingsupervision.europa.eu/press/blog/2025/html/ssm.blog20250603~7af4ffc2d7.en.html#footnote.7

15. House of Lords, *Corrected oral evidence: Growth of private markets in the UK following reforms introduced after 2008*, October 2025, https://committees.parliament.uk/oralevidence/16572/html/

16. BoE, *Bank of England launches system-wide exploratory scenario exercise focused on private markets*, December 2025, https://www.bankofengland.co.uk/news/2025/december/boe-launches-system-wide-exploratory-scenario-exercise-focused-on-private-markets

17. BoE, *Funded realignment: balancing innovation and risk – speech by Vicky White*, September 2025, https://www.bankofengland.co.uk/speech/2025/september/vicky-white-speech-at-the-bank-of-america-annual-ceo-conference

18. Australia Securities & Investments Commission, *Advancing Australia's evolving capital markets: Discussion paper response report*, November 2025, https://download.asic.gov.au/media/1oppyq1e/rep823-published-5-november-2025.pdf

19. US Department of the Treasury, *Minutes of the Financial Stability Oversight Council*, June 2025, https://home.treasury.gov/system/files/261/FSOC-20250604-Minutes.pdf.

20. US Department of the Treasury, *Minutes of the Financial Stability Oversight Council*, June 2025, https://home.treasury.gov/system/files/261/FSOC-20250604-Minutes.pdf

21. European Commission, *targeted consultation on the application of the market risk prudential framework*, November 2025, https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-application-market-risk-prudential-framework_en

22. BoE, *CP17/25 – Basel 3.1: Adjustments to the market risk framework*, July 2025, https://www.bankofengland.co.uk/prudential-regulation/publication/2025/july/basel-3-1-adjustments-to-the-market-risk-framework-consultation-paper

23. European Commission, *AI Digital Omnibus proposal*, November 2025, https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

24. Pending legislative negotiations on the AI Digital Omnibus proposal.

25. Congress.Gov, *H.R.4801 - Unleashing AI Innovation in Financial Services Act*, July 2025, https://www.congress.gov/bill/119th-congress/house-bill/4801/text

26. Colorado Division of Insurance (CDI), *Notice of adoption – Amended Regulation 10-1-1 Governance and Risk Management Framework requirements for insurers' use of external consumer data and information sources, algorithms, and predictive models*, August 2025, https://doi.colorado.gov/announcements/notice-of-adoption-new-regulation-10-1-1-governance-and-risk-management-framework; Deloitte, *Colorado governance and risk management framework rule for insurers using AI/ECDIS*, August 2025, https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/consulting/2025/us-colorado-ai-ecris-governance-and-risk-framework-august-2025.pdf?icid=mosaic-grid_colorado-governance-and-risk-management-framework-rule-for-insurers-using-ai-ecdis; Department of Financial Services, *Industry Letter*, October 2025, https://www.dfs.ny.gov/industry-guidance/industry-letters/il20251021-guidance-managing-risks-third-party

27. Japan's growth is expected to slow from 1.1% (2025) to 0.7% (2026 projection) while Emerging and Developing Asia growth is projected to decline from 5.4% (2025) to 5.0% (2026 projection). ASEAN 5 is expected to maintain 4.2% growth (2026 projection), same as 2025. IMF, World Economic Outlook Update, January 2026: Global Economy: Steady amid Divergent Forces; World Economic Outlook 2026/003

28. IMF, *Outlook for Asia and the Pacific*, October 2025, Outlook for Asia and the Pacific

29. WTO, *Global Trade Outlook and Statistics*, October 2025, Global Trade Outlook and Statistics

30. Ibid.

31. European Commission, *Carbon Border Adjustment Mechanism*, Carbon Border Adjustment Mechanism

32. European Council, EU deforestation law: Council and Parliament reach a deal on targeted revision, 4 December 2025

33. Data Track, *China: Consumer Confidence Index (CCI)*, December 2025, China: Consumer Confidence Index (CCI) | DataTrack

34. The Conference Board, *The Conference Board Leading Economic Index® (LEI) for the US Declined in Both October and November*, January 2026, US Leading Indicators

35. ABC News, *China's trade surplus tops $US1 trillion as exports to Europe, Australia, South-East Asia surge*, December 2025, China's trade surplus tops $US1 trillion as exports to Europe, Australia, South-East Asia surge

36. World Economic Forum, *What's led to China's property-market woes and what does that mean for the world?*, September 2023, What's led to China's property-market woes and what does that mean for the world?

37. Asia Society, *Malaysia's Gamble: Turning Data Centres Into Industrial Power*, January 2026, Malaysia's Gamble: Turning Data Centres Into Industrial Power | Asia Society

38. NIQ, *Southeast Asia's consumers are redefining value amidst headwinds, powering a $5 trillion consumption future by 2035*, November 2025, Southeast Asia's consumers are redefining value amidst headwinds, powering a $5 trillion consumption future by 2035

39. UOB Private Bank, *BCG, National University of Singapore, The Asia Generational Wealth Report 2025: Succession in a New Era*, November 2025, The Asia Generational Wealth Report 2025: Succession in a New Era

40. Deloitte, *The Family Office Insights Series - Asia Pacific Edition - The Top 10 Family Office Trends*, 2024, https://www.deloitte.com/content/dam/assets-shared/docs/services/deloitte-private/2024/family-office-trends-asia-pacific-edition-report.Pdf

41. Ministry of Science and ICT (MSIT), *AI Basic Act*, December 2024 Press Releases - 과학기술정보통신부 >

42. Government of Vietnam, *Law on Artificial Intelligence*, December 2025, https://vanban.chinhphu.vn/?pageid=27160&docid=216334&classid=1&typegroupid=3

43. Regulations.ai, *Thailand – AI Law Principles (2025)*, June 2025, Draft Principles for AI Legislation (Draft Principles of the AI Law) - Thailand | Regulations.AI - The Site on AI Laws and Regulations | Regulations.ai

44. Ministry of Digital Affairs, *Legislative Yuan Passes Artificial Intelligence Fundamental Act in Third Reading, Laying Foundation for AI Innovation, Security Governance in Taiwan*, December 2025 https://moda.gov.tw/en/press/press-releases/18316

45. Government of the Republic of China, *Basic Law on Artificial Intelligence*, December 2025, https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=H0160093&kw=%e4%ba%ba%e5%b7%a5%e6%99%ba%e6%85%a7%e5%9f%ba%e6%9c%ac%e6%b3%95

46. Cyberspace Administration of China, *Interim Measures for the Administration of Generative Artificial Intelligence*, July 2023 生成式人工智能服务管理暂行办法_中央网络安全和信息化委员会办公室

47. National Standards of the People's Republic of China, *Cybersecurity technology—Basic security requirements for generative artificial intelligence service*, April 2025 标题

48. National Standards of the People's Republic of China, *Cybersecurity technology—Generative artificial intelligence data annotation security specification*, April 2025 标题

49. National Standards of the People's Republic of China *Cybersecurity technology—Security specification for generative artificial intelligence pre-training and fine-tuning data*, April 2025 标题

50. Japan Government, *Act on Promotion of Research and Development and Utilization of Artificial Intelligence-related Technologies*, May 2025 e-Gov Statute Search

51. Australia Government, Department of Industry Science and Resources, *National AI Plan*, December 2025 National AI Plan | Department of Industry Science and Resources

52. Australia Government, *Department of Industry Science and Resources, Guidance for AI Adoption*, October 2025 Guidance for AI Adoption | Department of Industry Science and Resources

53. Government of India, Ministry of Electronics and Information Technology, *AI Governance Guidelines Enabling Safe and Trusted AI Innovation*, November 2025 Final Version 01

54. AI Verify Foundation, *Global AI Assurance Pilot, 2025,* About Us – Global AI Assurance Pilot

55. Infocomm Media Development Authority, *Model AI Governance Framework for Agentic AI*, January 2026, imda.gov.sg/-/media/Imda/files/about/emerging-tech-and-research/artificial-Intelligence/mgf-for-age...

56. New Zealand Government, *Responsible AI Guidance for Businesses Investing with confidence*, July 2025 Responsible AI guidance for businesses

57. ASIC, *ASIC Chair Joe Longo – speech at the Australia Banking Association Banking Conference, AI: A blueprint for better banking?,* July 2025 AI: A blueprint for better banking? | ASIC

58. APRA, *APRA Executive Director of Cross-industry Risk, Chris Gower – speech to RMA CRO Conference*, September 2025, https://www.apra.gov.au/news-and-publications/apra-executive-director-of-cross-industry-risk-chris-gower-%E2%80%93-speech-to-rma

59. Japan Financial Services Agency, *AI Discussion Paper (Version 1.0): Preliminary Discussion Points for Promoting the Sound Utilization of AI in the Financial Sector*, March 2025, aidp_en.pdf

60. Japan Financial Services Agency, *AI Discussion Paper Version 1.0 – summary document*, March 2025, aidp_summary_en.pdf

61. Hong Kong Monetary Authority, *Generative Artificial Intelligence Sandbox – Practical Insights Report,* October 2025, HKMA Banking Regulatory Document Repository

62. Bank Negara Malaysia, *Regulatory Sandbox webpages,* Regulatory Sandbox - Bank Negara Malaysia

63. Bank Negara Malaysia, *Artificial Intelligence in the Malaysian Financial Sector*, August 2025, DP_Artificial_Intelligence_in_the_Financial_Sector.pdf

64. Monetary Authority of Singapore, *Consultation Paper on Guidelines on Artificial Intelligence Risk Management*, November 2025, final_consultation_paper_on_guidelines_on_ai_risk_management_forrelease.pdf

65. Reserve Bank of New Zealand, *Rise of the machines - How could artificial intelligence impact financial stability?,* May 2025, Rise of the machines - Reserve Bank of New Zealand - Te Pūtea Matua

66. Fintech Global, *New Zealand FMA targets AI, tokenisation, advice access*, August 2025, New Zealand FMA targets AI, tokenisation, advice access

67. IBM, *What is quantum computing?,* What Is Quantum Computing? | IBM

68. World Economic Forum, *Quantum leaps: 3 ways banks can harness next-gen technologies for financial services*, July 2025, Banking in the quantum technologies era: 3 strategic shifts to watch | World Economic Forum

69. Monetary Authority of Singapore, *MAS Collaborates with Banks and Technology Partners on Quantum Security*, August 2024, MAS Collaborates with Banks and Technology Partners on Quantum Security

70. Monetary Authority of Singapore, *MAS and Industry Partners Publish Technical Report on Proof-of-Concept Sandbox for Quantum-Safe Communications within the Financial Sector*, September 2025, MAS and Industry Partners Publish Technical Report on Proof-of-Concept Sandbox for Quantum-Safe Communications within the Financial Sector

71. Hong Kong Monetary Authority, *The HKMA Unveils "Fintech 2030" at the Hong Kong FinTech Week 2025*, November 2025, Hong Kong Monetary Authority - The HKMA Unveils "Fintech 2030" at the Hong Kong FinTech Week 2025

72. Australian Signals Directorate, *Planning for post-quantum cryptography*, September 2025, Planning for post-quantum cryptography (September 2025).pdf

73. Japan Financial Services Agency, *Main Topics Raised by the Financial Services Agency (FSA) at a Dialogue Meeting with the Industry Association*, June 2025, 02.pdf

74. Deloitte Asia Pacific Centre for Regulatory Strategy, *Safeguarding Data Privacy in AI: Balancing Innovation against Risk, and Ethical Challenges",* October 2025, safeguarding-data-privacy-ai-new.pdf

75. Consensus, *APAC Digital Asset Adoption 2025: Stablecoins, Tokenization & Integration*, November 2025, APAC Digital Asset Adoption 2025: Stablecoins, Tokenization & Integration

76. AMINA Group, *Hong Kong Leads APAC Digital Asset Adoption in 2025*, November 2025, Hong Kong Leads APAC Digital Asset Adoption in 2025 - AMINA Bank

77. United States of America Congress, *H.R.3633 – Digital Asset Market Clarity Act of 2025*, September 2025, Text - H.R.3633 - 119th Congress (2025-2026): Digital Asset Market Clarity Act of 2025 | Congress.gov | Library of Congress

78. Bank for International Settlements, *BIS Bulletin No 108 Stablecoin growth – policy challenges and approaches*, July 2025, Stablecoin growth - policy challenges and approaches

79. Leika Kihara (Reuters), *World's first yen-pegged stablecoin debuts in Japan*, October 2025, World's first yen-pegged stablecoin debuts in Japan | Reuters

80. Australian Treasury, *Treasury Laws Amendment (Regulating Digital Asset, and Tokenised Custody, Platforms) Bill 2025 Exposure Draft*, September 2025, Exposure draft bill: Treasury Laws Amendment Bill 2025: Digital asset, and tokenised custody, platforms

81. Australia Treasury, *Treasury Laws Amendment Bill 2025: Payments System Modernisation — amendment of the Corporations Act 2001 Exposure Draft*, October 2025, Exposure draft: Treasury Laws Amendment Bill 2025: Payments System Modernisation—amendment of the Corporations Act 2001

82. Australian Government, *Corporations Act 2001*, July 2019, Corporations Act 2001 - Federal Register of Legislation

83. ASIC, *ASIC Corporations (Stablecoin Distribution Exemption) Instrument 2025/631*, September 2025, ASIC Corporations (Stablecoin Distribution Exemption) Instrument 2025-631

84. Bloomberg, *South Korea's Ruling Party Unveils Plan to Allow Stablecoins*, June 2025, South Korea's Ruling Party Unveils Plan to Allow Stablecoins – Bloomberg

85. Hong Kong Government, *Cap.656 Stablecoins Ordinance*, August 2025, Cap. 656 Stablecoins Ordinance

86. HKMA, *Explanatory Note on Licensing of Stablecoin Issuers*, July 2025, Explanatory Note on Licensing of Stablecoin Issuers

87. HKMA, *Guideline on Supervision of Stablecoin Issuers*, August 2025, Guideline_on_supervision_of_licensed_stablecoin_issuers_eng.pdf

88. HKMA, *Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT Guideline)*, August 2025, Guideline_on_Anti-Money_Laundering_and_Counter-Financing_of_Terrorism_For_Licensed_Stablecoin_Issuers_eng.pdf

89. Hong Kong SAR Government - Council Business Divisions Legislative Council, *Policy Pulse Issue 10: Latest developments in fintech Policy Pulse and digital assets in Hong Kong*, October 2025, pp2025-10-latest-developments-In-fintech-and-digital-assets-in-hong-kong-e.pdf

90. People's Bank of China, *中国宏观审慎管理体系的建设实践与未来演进* October 2025, 中国宏观审慎管理体系的建设实践与未来演进

91. People's Bank of China, *A Joint Meeting convened to Curb Speculations in Virtual Currency Trading*, November 2025, A Joint Meeting convened to Curb Speculations In Virtual Currency Trading

92. Hélène Rey (International Monetary Fund), *Stablecoins, Tokens, and Global Dominance*, September 2025, Stablecoins, Tokens, and Global Dominance

93. The State Council of The People's Republic of China, *China's Digital RMB Transactions Top 14.2 Trillion Yuan*, October 2025, China's digital RMB transactions top 14.2 trillion yuan

94. Hong Kong Monetary Authority, *e-HKD Pilot Programme - Phase 2 Report*, October 2025, e-HKD_Pilot_Programme_Phase_2_Report.pdf

95. Bank of Korea, Central Bank Digital Currencies – 1st Proof of Concept Experiments, November 2022, | Central Bank Digital Currency(목록) | Topics | Bank of Korea

96. Reserve Bank of Australia, *Project Acacia: RBA and DFCRC announce chosen industry participants and ASIC provides regulatory relief for tokenised asset settlement research project*, July 2025, Project Acacia: RBA and DFCRC announce chosen industry participants and ASIC provides regulatory relief for tokenised asset settlement research project | Media Releases | RBA

97. Hong Kong Monetary Authority, *HKMA announces the new phase of Project Ensemble to support real-value transactions in tokenised deposits and digital assets*, November 2025, Hong Kong Monetary Authority - HKMA announces the new phase of Project Ensemble to support real-value transactions in tokenised deposits and digital assets

98. Monetary Authority of Singapore, *Foreign Exchange – Use of Tokenised Bank Liabilities for Transaction Banking*, July 2025, project-guardian-fx-workstream-transaction-banking.pdf

99. Monetary Authority of Singapore, *Asset and Wealth Management – Operationalising Tokenised Funds*, November 2025, project-guardian operationalising-tokenised-funds.pdf

100. Monetary Authority of Singapore, *Fixed Income – Fixed Income Framework*, November 2025, guardian-fixed-income-framework-v1_1.pdf

101. Government of Australia, *Corporations Amendment (Digital Assets Framework) Bill 2025*, November 2025, Corporations Amendment (Digital Assets Framework) Bill 2025 – Parliament of Australia

102. Securities and Futures Commission, *"A-S-P-I-Re" for a brighter future - SFC's regulatory roadmap for Hong Kong's virtual asset market*, February 2025, ASPIRe-roadmap-for-Hong-Kongs-virtual-asset-market-Eng.pdf

103. Australian Treasury, *Summary of consultation outcomes - Corporations Amendment (Digital Asset Framework) Bill 2025*, February 2026, https://storage.googleapis.com/files-autreasury/treasury/p/prj37f059c66284c24051948/page/c2025_701519_outcomes.pdf

104. Securities and Futures Commission, *Circular to virtual asset trading platforms on licensing process and revamped Second-phase Assessment*, December 2024, Circular to new virtual asset trading platforms seeking to be licensed – Enhanced licensing process and revamped external assessments | Securities & Futures Commission of Hong Kong

105. Securities and Futures Commission, *Circular on staking services provided by virtual asset trading platforms*, April 2025, Circular on staking services provided by virtual asset trading platforms | Securities & Futures Commission of Hong Kong

106. Hong Kong Monetary Authority, *Provision of Staking Services for Virtual Assets from Custodial Services*, April 2025, Provision of Staking Services for Virtual Assets from Custodial Services

107. Hong Kong Monetary Authority, *Supervisory Policy Manual CRP-1 - Classification of Cryptoassets*, September 2025, Cryptoassets standard: consultation on new and revised SPM modules and code of practice Enclosure : CRP-1 Classification of Cryptoassets

108. Bank for International Settlements, *Prudential treatment of cryptoasset exposures*, December 2022, Prudential treatment of cryptoasset exposures

109. Bank for International Settlements, *Cryptoasset standard amendments*, July 2024, Cryptoasset standard amendments

110. Hong Kong Government, *Banking (Capital) (Amendment) Rules 2025*, July 2025, The Government of the Hong Kong Special Administrative Region Gazette

111. Hong Kong Government, *Banking (Exposure Limits) (Amendment) Rules 2025*, July 2025, The Government of the Hong Kong Special Administrative Region Gazette

112. Financial Services and the Treasury Bureau, *Public Consultation on Legislative Proposal to Regulate Virtual Asset Custodian Services*, June 2025, VACUSTODY consultationn paper en.pdf

113. People's Bank of China, 打击虚拟货币交易炒作工作协调机制会议召开, November 2025, 打击虚拟货币交易炒作工作协调机制会议召开

114. Monetary Authority of Singapore, *Consultation Paper on the Prudential Treatment of Cryptoasset Exposures and Requirements for Additional Tier 1 and Tier 2 Capital Instruments for Banks*, March 2025, Consultation Paper on the Prudential Treatment of Cryptoasset Exposures and Requirements for Additional Tier 1 and Tier 2 Capital Instruments for Banks

115. Monetary Authority of Singapore, *Guidelines on Licensing for Digital Token Service Providers*, May 2025, Guidelines on Licensing for Digital Token Service Providers

116. Securities and Exchange Commission, Thailand, *SEC adds USDC and USDT to the cryptocurrencies list*, March 2025, English (United States) News Detail

117. Securities and Exchange Commission, Thailand, *SEC amends regulations to exempt digital asset fund manager licenses for SCs and AMCs managing digital asset investments under securities regulations*, March 2025, English (United States) News Detail

118. Securities and Exchange Commission, Thailand, *SEC updates collaborative efforts with digital asset business operators to combat mule accounts*, March 2025, English (United States) News Detail

119. Securities and Exchange Commission, Thailand, *SEC launches TouristDigiPay, business operator applications start 25 September 2025*, September 2025, English (United States) News Detail

120. Secretariat, *Global Financial and Economic Crime Outlook 2025*, April 2025, Global Financial and Economic Crime Outlook 2025 - Secretariat

121. Adetunji Adejumo Paul and Chinonso Ogburie, *The Role of AI in preventing financial fraud and enhancing compliance*, March 2025, The Role of AI in preventing financial fraud and enhancing compliance | GSC Advanced Research and Reviews

122. Australian Government, *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025*, August 2025, Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 - Federal Register of Legislation

123. The State Council of the People's Republic of China, *China revises Anti-Money Laundering Law*, November 2024, China revises Anti-Money Laundering Law

124. Financial Action Task Force, *Global Assessment Calendar*, Assessments

125. Japan Financial Services Agency, *Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks*, March 2025, 01.pdf

126. Monetary Authority of Singapore, *National Anti-Money Laundering Strategy Singapore*, October 2024, singapore-national-aml-strategy.pdf

127. Monetary Authority of Singapore, *COSMIC*, COSMIC

128. International Organization of Securities Commissions, *IOSCO's Statement on Combatting Online Harm and the Role of Platform Providers*, May 2025, IOSCO's Statement on Combatting Online Harm and The Role of Platform Providers

129. Australian Securities & Investments Commission, *Scammers on notice as ASIC steps up action to protect consumers from online investment scams*, August 2025, 25-171MR Scammers on notice as ASIC steps up action to protect consumers from online investment scams | ASIC

130. Securities and Futures Commission, *SFC welcomes IOSCO's statement on combatting online scams*, May 2025, SFC welcomes IOSCO's statement on combatting online scams | Securities & Futures Commission of Hong Kong

131. Securities and Exchange Board of India, *SEBI Intensifies Efforts to Combat Online Investment Scams, Calls for Greater Collaboration from Social Media Platforms*, November 2025, SEBI | SEBI Intensifies Efforts to Combat Online Investment Scams, Calls for Greater Collaboration from Social Media Platforms

132. Indonesia Financial Services Authority, *The Rise of Scams, OJK and the Government Launch National Campaign to Combat Scam and Illegal Financial Activities*, August 2025, Press Release: The Rise of Scams, OJK and the Government Launch National Campaign to Combat Scam and Illegal Financial Activities

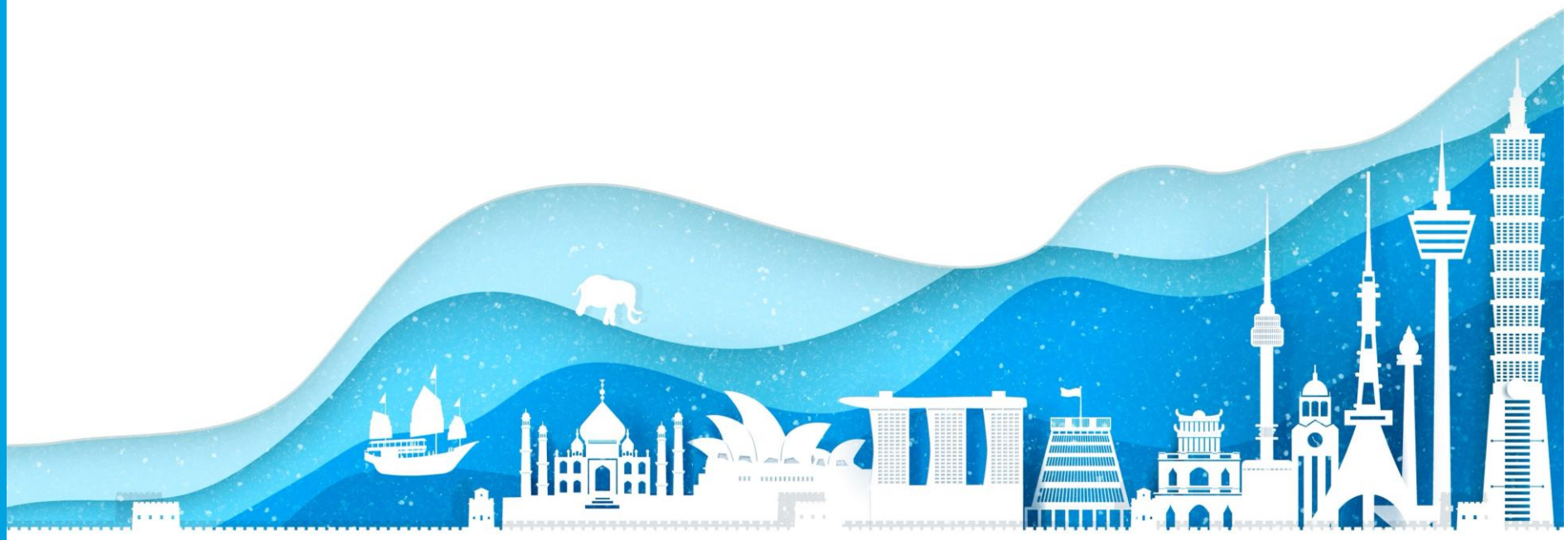
133. Financial Services Commission, *AI-based Anti-phising Sharing and Analysis Platform (ASAP) Launched to Bolster Protection against Financial Scams*, October 2025, Press Releases - Financial Services Commission

134. Monetary Authority of Singapore, *Joint press release by SPF, MAS, IMDA and GovTech on restricting access to facilities for scam mules*, September 2025, Joint press release by SPF, MAS, IMDA and GovTech on restricting access to facilities for scam mules

135. Australian Government, *Fintel Alliance*, Fintel Alliance | AUSTRAC

136. Hong Kong Monetary Authority, *Fraud and Money Laundering Intelligence Taskforce launched*, May 2017, Hong Kong Monetary Authority - Fraud and Money Laundering Intelligence Taskforce launched

137. Monetary Authority of Singapore, *AML/CFT Industry Partnership (ACIP)*, AML/CFT Industry Partnership (ACIP)



Deloitte.

The Deloitte Centre for Regulatory Strategy is a source of critical insights and advice, designed to assist the world's largest financial institutions manage the strategic and aggregate impact of regional and international regulatory policy. With regional hubs in Asia Pacific, the Americas and EMEA, the Centre combines the strength of Deloitte's 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.

Designed by CoRe Creative Services. RITM2380924