Deloitte.



Centre for Regulatory Strategy Asia Pacific

Frontier Technology Regulatory Updates in Financial Services

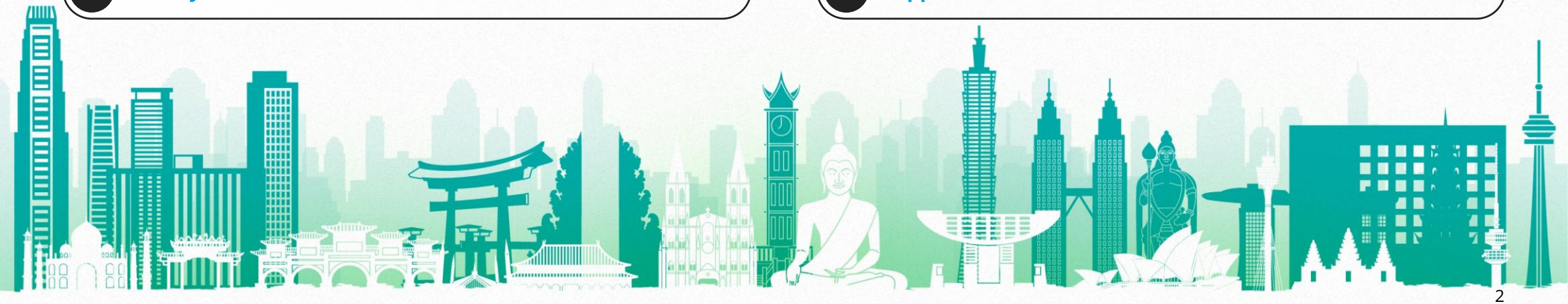
Q3 2026

November 2026

Table of Content

Click icon to navigate to the relevant section

1	Executive Summary	3 - 7
2	Australia	8 - 11
3	China Mainland	12 - 17
4	Hong Kong SAR	18 - 22
5	India	23 - 25
6	Indonesia	26 – 30
7	Japan	31 - 35
8	Malaysia	36 - 41
9	New Zealand	42 - 43
10	Philippines	44 - 49
11	Singapore	50 - 54
12	Taiwan (China)	55 - 58
13	Thailand	59 - 65
14	Vietnam	66 - 68
15	Contacts	69 - 70
16	Appendix	71 - 81



Executive Summary

The Deloitte Asia Pacific Centre for Regulatory Strategy (ACRS) is pleased to share the first edition of frontier technology regulatory updates in financial services. This publication brings together selected developments in artificial intelligence (AI), cyber resilience, digital identity, digital assets and quantum computing affecting financial institutions across Asia Pacific (AP) during the third quarter (Q3) of 2026. It covers both financial-sector measures and wider policy, legal and regulatory developments relevant to the industry.

Key developments this quarter included:

1. AI governance and controlled experimentation
Legislative proposals in both Malaysia and the Philippines share an emphasis on establishing mandatory, risk-based AI governance frameworks under central regulatory oversight. Malaysia's National AI Office consulted on a proposed AI Governance Bill that would introduce a central authority and a risk-based framework including an 'unacceptable' risk category. The Malaysia Securities Commission also consulted on board oversight of technology and disclosures on the use and governance of technology and AI by publicly listed companies. In the Philippines, the proposed Artificial Intelligence Regulation Act would establish a National AI Commission and mandate system registration while also requiring developers and deployers to implement mechanisms for immediately halting any AI system that autonomously exceeds its intended function. Alongside this legislative track, the Bangko Sentral ng Pilipinas (BSP) issued its voluntary Governance Principles for Artificial Intelligence in Financial Services. These principles extend to third-party vendors and outsourced partners under a shared-responsibility model.

Australia announced plans to introduce national AI standards to regulate large data centres and frontier AI training, alongside establishing an office of AI. Under the proposed tiered framework, large data centres would face mandatory requirements governing energy efficiency, renewable sourcing, sustainable water consumption and workforce skills and training. Meanwhile, frontier AI labs authorised to conduct large-scale training in Australia would be subject to proposed minimum security and safety expectations, including the mandatory reporting of defined AI incidents. Alongside this infrastructure focus, the government outlined broader consumer safety priorities, including a proposed digital duty of care, privacy reforms, workplace safety measures and the examination of consumer-law options to address risks arising from automated, agentic transactions. On the market side, the Australian Securities and Investments Commission (ASIC) amended its Market Integrity Rules to strengthen safeguards for algorithmic and AI-enabled trading, including controls enabling the immediate suspension, limitation or prohibition of trading involving particular algorithms. The amended requirements will commence on 18 March 2028. Japan's second AI Basic Plan addresses the expansion of agentic AI through design safeguards, improved AI literacy and a strategic focus on 'AI sovereignty' to avoid excessive dependence on any particular country or company.

This focus on the systemic risks of autonomous systems is mirrored in Taiwan, where the Ministry of Digital Affairs (MODA) launched its AI Risk Taxonomy and Assessment Framework (v1.0) to serve as a common standard for sectoral regulators, including the Financial Supervisory Commission (FSC), to draft industry-specific rules. The advisory framework groups 20 risk sub-types into technical, operational and societal categories. Under the operational category, the framework explicitly addresses agentic AI through a dedicated sub-type: 'unauthorised actions by autonomous AI agents'. This sub-type flags the risk of agents autonomously acquiring system access beyond their authorised scope or triggering unpredictable multi-agent chain reactions. Rather than imposing static risk tiers, it guides sectoral regulators through a four-step regulatory cycle: compiling an inventory of use cases, identifying risks against the 20 sub-types, assessing risks and implementing proportional responses.

In Singapore, the Monetary Authority of Singapore (MAS) published the industry-developed Safeguards for Agentic Finance at Runtime (SAFR) white paper, proposing runtime governance checkpoints to verify and record AI agents' proposed actions before execution. This was accompanied by the Personal Data Protection Commission (PDPC) finalising its Advisory Guidelines on Use of Personal Data in Generative AI, clarifying data protection responsibilities across model training, fine-tuning and retrieval-augmented generation (RAG). The Infocomm Media Development Authority (IMDA) also issued voluntary Transparency Guidelines for Generative AI Chatbots.
Hong Kong's financial regulators selected 36 use cases for the first Generative AI Sandbox++ cohort to test agentic applications, including testing how AI can oversee other AI applications. Separately, the Office of the Privacy Commissioner for Personal Data (PCPD) published dedicated guidance on agentic AI, warning that autonomous agents pose higher data privacy risks than standard chatbots and recommending a human-in-the-loop approach for decisions likely to have a significant impact on individuals, alongside minimum access controls.

Elsewhere in the region, New Zealand's Financial Markets Authority launched a thematic review of AI in financial advice, while Standards New Zealand consulted on adopting 14 international AI standards, including the joint International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standard ISO/IEC 38507 on the governance implications of organisational use of AI.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Executive Summary

2. Cyber resilience against AI-enabled threats
Regulators in Australia, Singapore, Taiwan and the Philippines issued warnings or mandated measures in response to concerns that frontier AI models could compress incident response windows by automating the identification and exploitation of software vulnerabilities. The Australian Prudential Regulation Authority (APRA) and ASIC highlighted how these capabilities shorten the time available to patch systems, calling on boards to establish clear escalation pathways, timely patching schedules, tested backups and recovery arrangements before a crisis occurs. Taiwan's Financial Supervisory Commission (FSC) highlighted 'Claude Mythos Preview' to illustrate frontier models' ability to identify vulnerabilities and generate attack code at scale, warning of shorter remediation windows and a 'patch flood' that could overwhelm institutional information technology (IT) resources. To counter these threats, in the Philippines, the BSP issued six recommendations, urging financial institutions to maintain accurate, up-to-date inventories of externally reachable assets and dependencies and to transition to phishing-resistant authentication, such as hardware security keys, for all administrative and privileged access.

While defensive AI can support vulnerability detection and incident response, regulators cautioned that these tools require governance and human oversight and cannot replace fundamental cyber hygiene. Regulators also emphasised the systemic risks associated with shared dependencies, where concentrated reliance on a few cloud, software as a service (SaaS) or AI model providers could escalate an isolated vendor disruption into sector-wide failure. For software-supply-chain risks, Taiwan's FSC recommended software bills of materials (SBOMs) to track third-party components, alongside contractually agreed patching service levels with critical suppliers.

In Singapore, MAS required key financial institutions to conduct AI-assisted red teaming on critical, internet-facing systems from 1 July 2026. MAS also announced the formation of the Association of Banks in Singapore's AI-Driven Cyber and Tech Risk Taskforce (ABS-ACT), comprising MAS and industry representatives. Additionally, MAS announced that it will soon issue supervisory expectations requiring key institutions to submit detailed assessments and action plans regarding their vulnerability detection, patching, testing, and recovery capabilities.

3. Preparing for quantum-related security risks
Measuring and building resilience against future quantum computers capable of breaking widely used public-key cryptography is an ongoing concern for regulators. The Hong Kong Monetary Authority (HKMA) launched its Whitepaper on Quantum Preparedness of Hong Kong's Banking Sector alongside its first Quantum Preparedness Index (QPI), which evaluates institutions across four dimensions: Awareness, Planning, Pilots and Practical Preparedness. The banking sector's initial baseline score was 2.3 on a ten-point scale. Although 68% of surveyed banks were at the awareness, planning or piloting stages, 32% had not yet begun their transition journey. Around half lacked formal post-quantum planning, only half had discussed the risk at board level, and one-third were exploring or piloting quantum-related technologies. HKMA Deputy Chief Executive Arthur Yuen warned that banks must transition to post-quantum cryptography (PQC) before the first active decryption attacks occur, noting that the HKMA will monitor individual bank QPI scores.

To support its goal of achieving full sectoral readiness (a QPI score of 10) by 2030, the HKMA is co-developing a PQC toolkit with the School of Business and Management of the Hong Kong University of Science and Technology (HKUST). The toolkit aims to build 'cryptographic agility', a capability recommended in the white paper that enables banks to upgrade cryptographic algorithms without major system disruption.

In Singapore, MAS stated its aim for financial institutions to achieve quantum resilience before the end of the decade. MAS announced that it would issue supervisory expectations later in 2026, with progressive milestones and timelines for institutions to compile inventories of cryptographic assets, prioritise the migration of vulnerable systems, and build technical capabilities and governance. MAS also committed SGD 220 million over three years under the renewed Financial Sector Technology and Innovation (FSTI 4.0) scheme. The scheme has six tracks, with quantum technology, AI and distributed ledger technology (DLT) among the priorities supported through its Institution Project track.

Executive Summary

4. Stronger authentication and fraud prevention
As generative AI increases risks from digital impersonation, supervisors strengthened authentication and fraud-prevention expectations. In Hong Kong, the Securities and Futures Commission (SFC) issued a circular expecting licensed internet brokers and SFC-licensed virtual asset service providers (VASPs) to implement phishing-resistant authentication, such as passkeys or robust device binding, for client logins and device registration or binding. The SFC stated that one-time passwords (OTPs) are not phishing-resistant and should not be used for these processes. Clients should generally register no more than three passkeys and/or three devices, with additional registrations permitted following adequate assessment. Firms must also monitor abnormal trading patterns, particularly following device changes or password resets, and report hacking incidents immediately. Robust authentication is expected as soon as practicable and no later than 8 July 2027, with immediate implementation by large internet brokers. Monitoring and response enhancements are expected immediately. The SFC will hold firms accountable for client losses where safeguards fail to prevent, detect and stop large-scale unauthorised transactions following hacking incidents.

Japan's JFSA updated its supervisory guidelines for insurers, moneylenders and payment firms to make phishing-resistant multifactor authentication (MFA), such as passkeys or certificate-based logins, the mandatory default for logging in, withdrawing funds or changing payee accounts. Where customers cannot use the necessary equipment, firms must provide alternative MFA and monitor the use of exceptions. To prevent credential harvesting, the JFSA also expects firms to remove login links from direct customer communications, such as emails and short message service (SMS) messages, except where no alternative is available, for example to fulfil a legal obligation.

Onboarding and biometric systems have also become key defensive frontiers. The HKMA updated its remote onboarding guidance for banks and stored value facility (SVF) licensees in response to AI-driven automation and deepfake attacks. It reaffirmed two existing core principles: Identity Authentication, using technology to verify electronic document reliability, and Identity Matching, using technology to link the customer conclusively to the identity provided. In Thailand, the Bank of Thailand (BOT) consulted on security guidelines for facial recognition used in mobile banking apps, targeting AI deepfakes, presentation attacks and video-injection attacks. The draft guidelines propose at least quarterly vulnerability assessments, annual penetration testing covering injection attacks, and performance metrics including a maximum False Match Rate (FMR) of 0.01% and a maximum Impostor Attack Presentation Accept Rate (IAPAR) of 4% for each attack type.
To support these technical controls, jurisdictions are reinforcing legal deterrents and cross-sector coordination. Taiwan's FSC amended its fraud-prevention regulations to enable cross-sector fraud-account inquiries involving deposit-taking institutions, payment firms and VASPs, and support shared anti-fraud platforms subject to approval. Malaysia's Parliament passed the Cybercrimes Bill 2026, including a synthetic-media offence in Clause 23 that would criminalise distributing deceptive computer-generated or manipulated audio or visual content with intent to commit or facilitate an offence, carrying a penalty of up to seven years' imprisonment or MYR 500,000 in fines.

5. Digital asset regulation and tokenisation
Regional regulatory developments on digital assets largely focused on supervision, financial crime controls and tokenised settlement infrastructure.

VASP licensing and stablecoin frameworks
Taiwan promulgated the Virtual Asset Service Act, establishing a comprehensive regulatory regime for seven activities, including exchange, custody, transfer and lending of virtual assets. Stablecoin issuance will require approval from the Central Bank and FSC, full reserve assets held in trust and public disclosures. The law provides for penalties of three to ten years' imprisonment for specified fraud and market-manipulation offences. Existing registered service providers will have 12 months from commencement to apply for a licence.

In Singapore, MAS consulted on amendments to the Payment Services Act 2019 to operationalise its Single-Currency Stablecoin (MAS-SCS) framework. Under the proposed framework, licensed Singapore-incorporated issuers may use the 'MAS-regulated stablecoin' label. The proposals would prohibit payment of interest to holders, require full reserve backing with segregated assets, and introduce regular stress testing. They also outline criteria for recognising a limited number of foreign-issued stablecoins under equivalent regulatory regimes and would permit jointly issued stablecoins subject to case-by-case exemptions and safeguards.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Executive Summary

Wholesale tokenisation and settlement infrastructure
Concurrently, jurisdictions are using tokenisation and wholesale digital currencies to modernise core settlement layers. In Australia, the Reserve Bank of Australia (RBA) launched a consultation on the role of the Reserve Bank Information and Transfer System (RITS) in supporting a tokenised financial ecosystem, building on Project Acacia's findings that tokenisation has the potential to improve wholesale market efficiency. Alongside this, the RBA and Treasury reaffirmed that there is currently no clear public interest case for a retail central bank digital currency (CBDC).

In the Philippines, the BSP highlighted findings from its Project Agila report detailing its wholesale CBDC proof of concept on Hyperledger Fabric. The pilot demonstrated round-the-clock transfer capability. In scalability tests, it processed 105,000 transactions in under 10 hours; further optimisation was needed at higher volumes. The report recommended focusing next on settling tokenised financial securities and institutional cross-border payments. In Hong Kong, following the June 2026 completion of the first phase of the DLT Fixed Income Review by the Financial Services and the Treasury Bureau (FSTB) and the HKMA, clarifications confirmed that debenture holders' registers maintained on DLT can meet the relevant Companies Ordinance record-keeping requirements. The Chief Executive's Policy Address outlined plans to test tokenised Exchange Fund Bills and promote trading of regulated stablecoins on licensed virtual asset trading platforms.

Financial crime controls and retail safeguards
To support this expanding digital ecosystem, regional regulators are tightening financial crime prevention rules and retail market safeguards. Thailand's Securities and Exchange Commission (SEC) proposed restricting stablecoin transfers to verified customer-owned accounts or wallets, with separate inbound and outbound limits of THB 5 million per customer per day per operator, subject to specified exemptions. This was accompanied by the formal issuance of Thailand's Travel Rule for Digital Assets, effective 27 February 2027. Draft rules for crypto exchange-traded funds (ETFs) would initially cover Bitcoin and Ethereum and primarily require Thai-licensed custodians. A related consultation proposed revised qualifications for foreign custodians serving digital asset funds, including a possible list of 11 jurisdictions.

In Vietnam, the National Assembly passed a law which will bring crypto-asset service providers into the AML regime from 1 December 2026. The law subjects providers to customer due diligence and record-keeping, and introduces 15 crypto-specific suspicious activity indicators, such as transaction splitting and the use of mixers. It also places existing restrictions on foreign-currency transactions, pricing, listings and quotations on a statutory basis, subject to authorised exceptions.

We invite you to read the full report for the detailed updates by jurisdiction, with other notable regional developments included in the appendix.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Frontier Technology Regulation

Key Developments in Q3 2026

Australia
- Prime Minister announced mandatory Australian Standards for data centres and frontier AI and established the Office of AI - July 2026
- APRA and ASIC Information Paper on Resilience to Frontier AI Risk – August 2026
- ASIC Corporate Plan 2026-27 prioritises AI adoption and frontier AI – August 2026
- ASIC amended Market Integrity Rules to strengthen safeguards for AI-enabled trading – September 2026

China (Mainland)
- CAC revision draft of the Internet Information Services Measures – July 2026
- TC260 Security Guide for Individual Users for AI Services – August 2026
- SPC Opinions on Adjudicating AI-Related Disputes – September 2026
- TC260 AI Application Security Guidelines – September 2026
- TC260 draft Security Guide for AI Agent System Development – September 2026

Hong Kong SAR
- SFC mandates phishing-resistant authentication for internet brokers and VASPs – July 2026
- HKMA, SFC, IA, and MPFA joint circular on the cross-sectoral cyber-mapping exercise – July 2026
- HKMA Quantum Preparedness Whitepaper and first Quantum Preparedness Index – July 2026
- PCPD guidance on protecting personal data in the use of agentic AI – August 2026
- Gen AI Sandbox++ first cohort focused on agentic AI – August 2026
- HKMA remote on-boarding guidance updated for AI-driven automation and deepfakes – September 2026

India
- RBI consults on data governance expectations – July 2026
- RBI consolidates cybersecurity and technology risk requirements into tiered Master Directions – July 2026

Indonesia
- OJK governance and risk management obligations for financial sector technology innovation (ITSK) providers in force – July 2026
- Government Regulation 33/2026 implementing the Personal Data Protection Law – July 2026 (effective January 2027)

Malaysia
- BNM Financial Technology Regulatory Sandbox Green Lane cohort opened – July 2026
- NAIO consultation on proposed AI Governance Bill – July 2026
- SC consulted on mandatory board-level AI governance disclosure – July 2026
- Cybercrime Bill 2026 criminalises malicious deepfakes; passed in July 2026, awaiting royal assent

Japan
- Draft Second AI Basic Plan centred on agentic AI and AI sovereignty published – July 2026
- JFSA sets phishing-resistant authentication expectations for insurers, money lenders, and payment firms – July 2026
- JFSA moves cyber incident reporting onto inter-agency common forms – September 2026

New Zealand
- Biometric Processing Privacy Code 2025 in full force – August 2026
- FMA thematic review of AI in financial advice opened – August 2026
- Standards New Zealand consults on adopting 14 international AI standards – August 2026

Philippines
- BSP recommendations for managing emerging risks from frontier AI systems – July 2026
- Proposed AI Regulation Act (AIRA) – July 2026

Singapore
- MAS requires AI-assisted red-teaming for key FIs – July 2026
- Safeguards for Agentic Finance at Runtime (SAFR) published – July 2026
- PDPC finalises Advisory Guidelines for Generative AI Chatbots – July 2026
- MAS and ABS taskforce set up to strengthen resilience against AI-driven threats – July 2026

Taiwan (China)
- MODA AI Risk Classification Framework – July 2026
- FSC challenges and strategy recommendations for responding to AI attacks – July 2026

Thailand
- BOT consults on security guideline for facial recognition against AI deepfake attacks – September 2026

Vietnam
- PM issued a List of High-Risk AI Systems – June 2026

**Please note this is meant for illustrative purposes only and does not include all AI related rules and guidelines*
*Jurisdictions coded **Green** have adopted a voluntary, principles-based approach to AI regulation, with AI risks otherwise addressed through existing laws and sector rules.*
*Jurisdictions coded **Blue** have adopted, proposed, or announced plans to introduce mandatory requirements for some AI systems or applications.*

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (1/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	PM	**Prime Minister Sets Out "AI in Australia's Interests" Agenda and Establishes an Office of AI**	On 15 July 2026, Prime Minister Anthony Albanese delivered "AI in Australia's Interests" at the University of Sydney, announcing plans for mandatory Australian Standards for artificial intelligence (AI). An Office of AI was established within the Department of the Prime Minister and Cabinet to coordinate the standards' design and AI work across government. The Government aimed to bring legislation to Parliament in early 2027. The proposed framework would cover large data centres and frontier AI training. Data-centre requirements would address location, energy and water use, including obligations to underwrite new power supply, meet grid connection costs, minimise water use and fund additional water infrastructure. The Prime Minister also committed to protecting Australian creators' ownership and control of works used to train AI. A September consultation proposed minimum security and safety expectations for frontier laboratories authorised to undertake large-scale AI training in Australia, including reporting defined AI incidents. It also sought views on contributions to domestic skills, research and innovation. Responses were invited by 9 October 2026. Separately, on 20 July, the Government outlined wider AI consumer-safety priorities: • **Digital duty of care**: legislate to require AI companies to build in safety by design and proactively address potential harm. • **Privacy:** consult on further reforms to strengthen, modernise and simplify personal data protection laws. • **Workplace safety:** pursue AI safety through the tripartite Artificial Intelligence Workplace and Employment Forum. • **Consumer protection:** examine options under Australian consumer law to address risks including retail surveillance **pricing and agentic commerce.** • **Government decision-making:** develop a framework to better regulate automated decision-making within federal agencies. Prime Minister Announces Australian Interests for AI and a New Office of AI | PM AI consumer safety priorities | The Hon Dr Andrew Charlton MP | Ministers for the Department of Industry, Science and Resources Getting it right: Building AI infrastructure that works for Australia: Consultation paper - September 2026 | PM&C	Office of AI established on 15 July 2026; and Legislation targeted for introduction to Parliament in early 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (2/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**APRA ASIC**	**APRA and ASIC Warn Frontier AI Awareness Must Turn to Action**	On 27 August 2026, the Australian Prudential Regulation Authority (APRA) and the Australian Securities and Investments Commission (ASIC) published the information paper "Resilience at Frontier AI Speed: Insights from the APRA-ASIC Industry Roundtables". It summarises nine roundtables on entity preparedness for frontier AI risk held in June and July 2026. The paper records that industry awareness of frontier AI risk is established. It identifies the operative question for boards and executives as whether their entities can make decisions, maintain critical operations and recover when incidents unfold faster, affect more parties and involve more complex dependencies. The regulators expect entities to demonstrate that key decisions, escalation pathways, recovery arrangements, assurance activities and governance processes can operate at the speed required, and state that this will remain a heightened supervisory focus. Key themes include: • **Cyber fundamentals:** frontier AI raises the cost of weak controls, placing weight on visibility of technology resources and attack surfaces, timely patching, identity and access controls, monitoring, backup integrity and tested recovery arrangements, and on identifying where legacy systems create vulnerabilities, constrain recovery options or complicate incident response; • **Governance and escalation:** board engagement has risen, and compressed incident timeframes leave limited room to escalate decisions or resolve competing priorities. Guardrails on risk appetite, escalation authority, supplier reliance, recovery priorities, communications and resilience investment therefore need settling before a crisis. Gaps in incident plans, escalation triggers and delegation arrangements can prove as disruptive as technical control failures; • **Defensive AI:** use of AI is growing across threat intelligence, vulnerability detection, code review and incident response, while governed, measurable and scalable capacity remains limited and does not displace strong cyber fundamentals. Defensive AI itself requires governance, accountability, secure configuration, monitoring, reliability testing and human oversight, and introduces new risks where poorly governed; • **Shared dependencies:** concentrated reliance on cloud, Software-as-a-Service, managed service providers, AI model providers, open-source components, payments infrastructure and telecommunications can spread an isolated incident across the sector. Readiness turns on knowing which providers support critical operations, where dependencies overlap, how disruption would propagate, and whether fallback, restoration and reconnection arrangements hold under compressed timeframes; and • **Collaboration:** interconnection both spreads disruption and supports resilience. Sector-wide threat intelligence sharing, dependency mapping, supplier assurance and incident coordination through industry associations supplement each entity's own accountabilities, which remain unchanged. Resilience across the system is limited by its least prepared participants. APRA and ASIC Warn Frontier AI Awareness Must Turn to Action | APRA Resilience at Frontier AI Speed - Insights from the APRA-ASIC Industry Roundtables | APRA and ASIC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (3/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	ASIC	**RBA Consults on the Role of its Settlement System in Supporting Tokenised Money and Assets**	On 3 September 2026, the Reserve Bank of Australia (RBA) launched a consultation on the role of the Reserve Bank Information and Transfer System (RITS) in supporting settlement within a tokenised financial ecosystem. The initiative follows findings from Project Acacia, which identified tokenisation as having the potential to improve the efficiency, functionality and resilience of Australia's wholesale financial markets. The RBA is seeking feedback on how its settlement services could support the development and growth of tokenised asset markets and tokenised private money, while continuing to promote safety, efficiency and financial stability. Alongside this initiative, the RBA and Treasury published "Retail Central Bank Digital Currency in the Australian Context: An Update". It concluded that Australia's retail payments system is functioning effectively and that there is currently no clear public interest case for a retail central bank digital currency (CBDC). The publications form part of the RBA's broader programme of work to ensure Australia's money, payments and settlement arrangements remain fit for the future. They are consistent with the conclusions of the 2024 joint RBA-Treasury paper on digital money and CBDCs in Australia. RBA Consults on Settling Tokenised Money Through Its Payments System and Rules Out a Retail Digital Currency | RBA	Public consultation ends on 30 October 2026. Broader public consultation on RITS Modernisation is expected in 2027.
4	ASIC	**ASIC Strengthens AI Trading Safeguards and Streamlines Market Integrity Rules**	On 24 September 2026, the Australian Securities and Investment Commission (ASIC) announced amendments to its Market Integrity Rules (MIRs) to strengthen safeguards for automated and AI-enabled trading, while simplifying regulatory requirements for securities and futures market participants. Key changes include: • Modernised trading system obligations reflecting current market practices and the risks associated with algorithmic trading, AI and machine learning; • Trading system requirements applied consistently across manually entered and automated orders; • Greater consistency between securities and futures market participant obligations; • Clarified scope of the false or misleading market conduct rule, including where AI-enabled trading creates a false or misleading appearance of the market; and • Alignment of Australia's market integrity framework with the principles and international standards of the International Organization of Securities Commissions (IOSCO) on algorithmic trading. Additionally, ASIC is consulting on proposed updates to Regulatory Guides 265 and 266, which would consolidate existing guidance, reduce regulatory complexity and withdraw Regulatory Guide 241. ASIC Strengthens AI Trading Safeguards and Streamlines Market Integrity Rules | ASIC Proposed Updates to RG 265 and RG 266 and Withdrawal of RG 241 | ASIC	Public consultation ends on 5 November 2026.

China Mainland



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (1/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	CAC	**CAC Consults on the Internet Information Services Measures to Add Platform and AI Service Rules**	On 3 July 2026, the Cyberspace Administration of China (CAC) opened a second public consultation on the Measures for the Administration of Internet Information Services (Revision Draft for Comment). The draft would fully revise the Measures in force since 2000. The CAC drafted it with the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS), then revised the first consultation text to reflect the amended Cybersecurity Law and public feedback. The proposed rules would cover anyone providing internet information services in China, including through websites, apps and AI agents, as well as overseas providers serving users in China. The draft would keep the existing licensing gateway: providers need approval or a telecom operating licence from the telecom authority, and news, finance, education and other regulated content services need sector approval first. It would also tighten controls on accounts. Providers would be required to verify users' real identities, restrict accounts that don't match a real identity or have been unused for more than six months, and keep logs for at least six months. Under a new section, platforms would publish their rules and assign each account a credit grade. They would also verify and label the credentials of public accounts producing content in fields such as finance, education and health. Large platforms are defined as those with more than 50 million registered users or 10 million monthly active users. They would need a dedicated compliance department and compliance officer, would handle complaints about unlawful content within 24 hours, and would report changes in major shareholders or actual controllers. A further new section would regulate providers that use AI to deliver internet information services. Key proposals include: • **Public disclosure** of the basic principles, purpose, main operating mechanism and training data sources of the AI technology used; • **Security assessment and algorithm filing** for services that can shape public opinion or mobilise the public; • **Training only on lawfully sourced data and foundation models**, with news services limited to state-approved news sources for training data; • **Labelling of AI-generated content** under mandatory national standards, with a ban on removing or altering labels; • An **option to receive recommendations not based on personal characteristics**, and a ban on forcing users onto intelligent services; • **Fair and transparent algorithms** for dispatching, assessing and paying workers; and • Use of AI agents that meet national requirements, with **safety management systems for agent services and agent distribution.** Finally, the draft would create a serious-dishonesty list for the internet sector. Listed parties could be barred from registering new accounts, have account functions restricted, or be banned from providing services. Fines would rise in tiers, reaching RMB 2 million to RMB 10 million for especially serious breaches of content, log-keeping, AI-labelling and large-platform obligations. Responsible individuals would face fines of up to RMB 1 million and possible bans from director and senior management roles. Notice of the Cyberspace Administration of China on Second Public Consultation on the Measures for the Administration of Internet Information Services (Revision Draft for Comment) | CAC	Public consultation ended on 2 August 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (2/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	TC260	**TC260 Publishes a Security Guide for Individuals Using AI Services**	On 24 August 2026, the Secretariat of the National Technical Committee 260 on Cybersecurity (TC260) published the Cybersecurity Standard Practice Guide – Security Guide for Individual Users of Artificial Intelligence Services (TC260-PG-20267A, v1.0), under notice Wang'an Mizi [2026] No. 105. The guide is a standards-related technical document that gives practical guidance. It is written for individuals who use AI services over the internet, especially services that make predictions, recommendations or decisions, or that generate text, images, audio and video. AI technology providers, developers and operators can also use it as a reference when helping individuals use their services safely. The guide has three parts: security awareness, safe-use measures and a code of conduct. It reminds users that AI can make errors, misread requests and produce false information. It also warns that AI can be misused to imitate relatives' voices or to fake official notices. For users who deploy AI agents, it points to the companion guide on agent deployment and use (TC260-PG-20266A). Key recommendations include: • Using AI services only from legitimate sources and, for generative AI, using models that have completed generative AI service filing, rather than unidentified relay sites or unauthorised proxies; • Checking user and privacy agreements for what personal data is collected and shared, whether inputs are used for training, and whether consent can be withdrawn; • Switching off unnecessary permissions, such as access to the microphone, camera, photo album and files; • Treating AI output on law, medicine, employment, education and financial management as reference only, and checking it through independent channels where money or personal safety is at stake; and • Keeping labels on AI-generated content intact, as set out in labelling standard GB 45438-2025, and not sharing generated content that is inaccurate or unlawful. Notice on Publishing the Cybersecurity Standard Practice Guide – Security Guide for Individual Users of Artificial Intelligence Services | TC260	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (3/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	SPC	**Supreme People's Court Issues China's First Judicial Rules on AI-Related Disputes**	On 7 September 2026, the Supreme People's Court (SPC) issued the Opinions on Lawfully Adjudicating Cases Involving Artificial Intelligence Disputes (Fa Fa [2026] No. 10). The SPC described the Opinions as the first judicial rules on AI disputes issued by a national supreme court to guide courts at all levels in civil, intellectual property and criminal cases involving AI. They draw on existing laws, including the Civil Code, the Personal Information Protection Law and the Anti-Unfair Competition Law. The SPC stated that the Opinions rest on three principles: putting people first, supporting innovation, and securing a safety baseline. Under the Opinions, liability for harm caused using AI is fault-based unless a law says otherwise. Courts weigh how autonomous, transparent and risky the application is, and what precautions its developers and providers took. Key rulings include: • **Creating an identifiable digital likeness or cloned voice of a person without consent** can infringe their portrait, name or voice rights, and an unauthorised digital recreation of a deceased person gives close relatives a claim; • **Training models on personal information** that was lawfully made public is generally not infringement if the individual has not clearly objected and the use stays within a reasonable scope, but uses with a significant impact on the individual's rights require consent; • **Generative AI providers are liable if they fail to stop generating infringing content** after a valid notice, while users who deliberately prompt infringing output bear primary liability; • Only physical products, such as robots and autonomous vehicles, are treated as products under product liability law, so purely digital AI services fall outside it; • **Using algorithms to charge consumers different prices** without good reason creates liability, and consumers can claim punitive damages where fake celebrity endorsements amount to fraud; and • **Developers who deny copyright infringement may need to disclose their training data sources** and process records, and only a natural person can be named as the inventor in an AI-related patent. On procedure, if a party holding key evidence refuses without good reason to produce it, courts may accept the other side's account of what that evidence shows. Parties who file AI-assisted court documents must check their citations and disclose that AI was used. Using AI to fabricate evidence or bring a sham lawsuit can lead to fines, detention or criminal liability. The SPC stated that it left two disputed questions out of the Opinions for further study: whether AI-generated output can be protected by copyright, and how to treat AI training on copyrighted works used without permission. Supreme People's Court Issues the Opinions on Lawfully Adjudicating Cases Involving Artificial Intelligence Disputes | SPC Officials of Relevant SPC Departments Answer Reporters' Questions on the Opinions on Lawfully Adjudicating Cases Involving Artificial Intelligence Disputes | SPC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (4/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	TC260	**TC260 Publishes Lifecycle Security Guidelines for AI Applications Across All Sectors**	On 15 September 2026, TC260 published four Cybersecurity Standard Practice Guides on AI application security under notice Wang'an Mizi [2026] No. 118. The set contains a cross-sector General Principles guide (TC260-PG-20268A, v1.0) and three sector guides, for education, health care, and broadcasting and online audiovisual services. TC260 stated that it prepared the guides to respond to new risks arising from the rapid development and use of AI. The General Principles apply to organisations in any sector that manage the security risks of AI applications, and regulators and third-party testing bodies may also use them as a reference. Organisations in a sector with its own guide are to meet both that guide and the General Principles. The Industrial and Commercial Bank of China and the Agricultural Bank of China were among the drafting organisations. The General Principles set out five principles, including final human control over AI and protection matched to each application's risk grade. They give guidance for seven lifecycle stages and assign responsibilities to data providers, builders and deployers, operators and users. Key guidance includes: • **Planning:** grade each application on a five-level scale running from low to especially serious risk, make sure each party's AI security capability is graded no lower than the application's risk, plan one-click takeover, rollback and emergency shutdown, and name a person with first responsibility for the application's security; • **Design and validation:** audit open-source frameworks and code, clean training data and guard it against poisoning, and test for harmful generated content, collisions by AI-controlled physical devices and the reliability of major decisions, with separate safeguards for minors; • **Deployment:** use guardrails against harmful content, prompt injection and loss of control over automated actions, encrypt data and use isolated containers on public cloud, and keep user data on the device unless the user consents; • **Operation:** label AI-generated content in line with GB 45438-2025, staff content reviewers in proportion to service size for services that shape public opinion, and keep emergency plans that include shutdown or switching to a backup service after a major incident; • **Ongoing evaluation:** repeat security testing every year and whenever risks change, and go back to the planning stage if the security design fails; and • **Retirement:** make models, model weights and user data unrecoverable when an application is withdrawn, and give users time to migrate before the service stops. Notice on Publishing Four Cybersecurity Standard Practice Guides Including the AI Application Security Guidelines – General Principles | TC260	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (5/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	TC260	**TC260 Consults on a Security Guide for Developing AI Agent Systems**	On 18 September 2026, TC260 opened a public consultation on the Cybersecurity Standard Practice Guide – Security Guide for AI Agent System Development (Draft for Comment, TC260-PG-2026NA, v1.0), under notice Wang'an Mizi [2026] No. 119. The draft would guide developers of software agent systems built on large models, whether they build them in-house, on a platform, with low-code or no-code tools, or by combining third-party models, tools and Model Context Protocol (MCP) services. Agents that mainly control physical devices, such as robots and self-driving vehicles, fall outside its scope. TC260 identifies prompt injection, drift away from the agent's set goals, abuse of permissions, data leakage, memory poisoning, supply chain weaknesses and cascading failures as the main risks agents face. The draft would arrange its security measures across five development stages. It rests on six principles, including risk-based and tiered controls, human control and end-to-end traceability. Key proposals include: • **Preparation:** set the limits of the agent's autonomy, the points where a human steps in and the actions the agent must never take, and record each risk in a risk register; • **Design:** use models that meet standard GB/T 45654-2025, give tools, plug-ins and MCP services only the access they need, cap execution steps, tool calls and resource use, and require human approval for high-risk or irreversible actions; • **Implementation:** run code and tools in isolated sandboxes, keep keys and access tokens out of code, prompts and logs, protect logs from tampering, and maintain an inventory of all software and AI components; • **Testing:** carry out red-team attacks covering prompt injection, memory poisoning, privilege escalation and multi-agent scenarios, and rerun tests whenever models, prompts or tools change; and • **Release:** confirm that security testing and fixes are complete before launch, roll out high-risk systems in stages, and repeat the security assessment after major changes such as replacing the underlying model. Notice on Public Consultation on the Cybersecurity Standard Practice Guide – Security Guide for AI Agent System Development (Draft for Comment) | TC260	Public consultation ended on 2 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	SFC	**SFC Mandates Phishing-Resistant Authentication and Suspicious Activity Surveillance for Internet Brokers and Virtual Asset Service Providers**	On 9 July 2026, the Securities and Futures Commission (SFC) issued a circular (26EC35, reference SFO/IS/021/2026) requiring licensed corporations engaged in internet trading and SFC-licensed virtual asset service providers (VASPs) to deploy phishing-resistant authentication and adequate monitoring and surveillance measures. The circular addresses licensed corporations holding Type 1, Type 2, Type 3 or Type 9 licences alongside VASPs; associated entities are not named in the addressee line. Firms must adopt passkeys based on public-key cryptography and device binding for client login. The SFC states expressly that it does not consider a one-time password to be a phishing-resistant authentication solution, and that internet brokers and VASPs should not use one for the processes covered. Transaction monitoring must flag abnormal trading patterns, unusual timing, large trades in illiquid stocks, and activity following password resets or device changes. Key requirements include: • Clients may not bind or register more than three passkeys and three devices for their internet trading accounts; • Client notification of successful logins, new device binding and suspicious activity must be delivered through multiple communication channels where applicable, such as email, SMS or push notification; • Hacking incidents must be reported to the SFC immediately, alongside containment, asset protection and client notification procedures; • The Manager-In-Charge of Overall Management and Oversight and the Manager-In-Charge of Information Technology are ultimately responsible for implementation; • The SFC states it will hold a firm accountable for client losses where measures are inadequate; and • No size-based exemption is provided. The SFC states it will take a pragmatic approach where systems require updating, and expects large internet brokers to implement immediately rather than at the outer deadline. SFC Mandates Phishing-Resistant Authentication and Suspicious Activity Surveillance for Internet Brokers and Virtual Asset Service Providers | SFC	Effective on 9 July 2026. Full authentication rollout deadline: 8 July 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**HKMA**	**HKMA Publishes Quantum Preparedness Whitepaper and First Sector Readiness Index for Banks**	On 27 July 2026, the Hong Kong Monetary Authority (HKMA) launched the Whitepaper on Quantum Preparedness of Hong Kong's Banking Sector together with the first Quantum Preparedness Index (QPI) and supporting measures, announced at the eighth edition of the FiNETech series and distributed to the banking sector as a circular titled Results of Quantum Preparedness Index Survey. Both were developed under the HKMA's Fintech Promotion Blueprint and are directed at the authorised institutions comprising Hong Kong's banking sector. The whitepaper reports a survey conducted in early 2026, from which the QPI is assessed across four dimensions — Awareness, Planning, Pilots and Practical Preparedness. The initial score is 2.3 on a ten-point scale. The HKMA states it will support the sector's transition to Post-Quantum Cryptography (PQC) with the aim of achieving full sectoral readiness, a QPI score of 10, by 2030 through practical guidance, training and industry engagement. Key findings include: • Around 68% of surveyed banks demonstrate awareness or are progressing to planning or piloting stages; 32% have not yet begun their transition journey; • Around half of surveyed banks have no formal post-quantum planning in place; • Around half of surveyed banks reported that quantum computing had been discussed at board level- About one-third of surveyed banks had begun exploring or piloting quantum-related initiatives; • A PQC toolkit is to be co-developed with the School of Business and Management of The Hong Kong University of Science and Technology and the industry, to assist banks in identifying transition planning priorities and enhancing cryptographic agility; and • A series of workshops is to follow on capability building and responsible use of quantum technologies. HKMA Publishes Quantum Preparedness Whitepaper and First Sector Readiness Index for Banks | HKMA Quantum Preparedness of Hong Kong's Banking Sector White Paper | HKMA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	PCPD	**PCPD Publishes Guidance on Protecting Personal Data Privacy in the Use of Agentic AI**	On 25 August 2026, the Office of the Privacy Commissioner for Personal Data (PCPD) published "Protecting Personal Data Privacy in the Use of Agentic AI", with the Digital Policy Office and the Hong Kong Applied Science and Technology Research Institute as supporting organisations. The guidance is directed at data users, including organisations and individuals. It supplements the PCPD's Artificial Intelligence: Model Personal Data Protection Framework, which the PCPD stated remains generally applicable to the use of agentic AI. Agentic AI is defined as an intelligent system with capabilities of autonomous perception, memory, decision-making, interaction and execution, built on foundation models integrated with tools such as databases, memory and computer operating systems. PCPD noted that AI agents are not legal persons and that organisations, as data users, remain accountable under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) and its six Data Protection Principles (DPPs). PCPD stated that agentic AI generally poses higher personal data privacy risks than ordinary AI chatbots. Key risks identified include: • **Extensive access:** higher default access rights to files, emails, account credentials and browser-stored contents, raising risks of unauthorised access, reproduction by third parties or accidental erasure; • **System vulnerabilities:** high access granted across multiple systems and data sources, so weaknesses in system design or safety controls affect personal data security; • **Vulnerable plugins or skills:** programmes not subject to rigorous security review may contain malicious code enabling account or system takeover; • **Function creep:** aggregation and recombination of data from multiple sources, including use for model training, beyond the original or a directly related purpose; and • **Multi-agent risks:** inaccurate or hallucinated data cascading between agents, amplified security risks, and complex data flows that impede access and correction rights. The guidance sets out nine recommendations mapped to the DPPs. These include • Avoiding excessive or arbitrary collection; • Transparency in Personal Information Collection Statements and Privacy Policy Statements; • Accuracy measures such as retrieval-augmented generation (RAG) and human review; and • Maximum retention periods for conversation histories, cache data and long-term memory. Also recommended are prescribed consent before any use for a new purpose; security measures including • Minimum access rights, plugin verification, large language model guardrails and logging for traceability; and • Privacy-by-design and privacy-by-default systems supporting access and correction rights. The remaining two recommendations are continuous risk assessment with a "human-in-the-loop" approach for high-stakes, irreversible or atypical actions, and an internal governance structure with allocated responsibilities, contractual controls over external vendors and staff training. PCPD stated that recommendations 1, 3, 4, 5 and 6 also apply to individual users, and that the Security Checklist in Annex A sets out practical steps across the evaluation, preparation, deployment, use and uninstall stages. PCPD Publishes Guidance on Protecting Personal Data Privacy in the Use of Agentic AI | PCPD Privacy Commissioner's Office Follows Up on Three Cases Involving Misuse of Employers' Personal Data by Foreign Domestic Helpers for Loan Applications and Publishes Guidance on "Protecting Personal Data Privacy in the Use of Agentic AI" | PCPD	-

Hong Kong SAR (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	HKMA	**HKMA Rewrites Its Remote On-boarding Guidance to Address AI-Driven Automation and Deepfake Attacks on Identity Verification**	On 3 September 2026, HKMA issued a circular (B10/1C, B1/15C and B10/21C) to authorised institutions (AIs) and stored value facility (SVF) licensees. It updates the HKMA's expectations for the remote on-boarding of individual customers in light of AI-driven automation and deepfakes, which the HKMA states increase impersonation, online fraud and mule-account risks. The circular supersedes the HKMA's circulars of 1 February 2019 and 24 May 2021 on remote on-boarding of individual customers and iAM Smart. Its circulars of 3 June 2020 on thematic review feedback and 24 September 2020 on remote on-boarding of corporate customers remain applicable and are to be read with it. The circular sets two core principles: • **Identity Authentication:** where identity information is obtained electronically, institutions should take appropriate measures, including technology, to ensure the reliability of the document, data or information used; and • **Identity Matching:** institutions should use appropriate technology to link the customer conclusively to the identity provided. AIs and SVF licensees are also expected to: • Maintain a continual programme of updates and recalibration for their remote on-boarding solutions; • Take a risk-based approach to product and service design, proportionate to each customer's assessed money laundering and terrorist financing risk; • Consider a tiered model, in which account features, functions and transaction limits are adjusted according to actual usage and ongoing customer behaviour; and • Ensure active senior management oversight. Institutions are further expected to carry out a comprehensive review of their remote on-boarding solutions, systems and oversight. The review should take into account the latest fraud and scam intelligence shared by the HKMA and the Hong Kong Police Force. HKMA Rewrites Its Remote On-boarding Guidance to Address AI-Driven Automation and Deepfake Attacks on Identity Verification | HKMA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

India



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

India (1/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	RBI	**RBI Consults on Data Governance Expectations Including a Single Source of Truth and a Senior Data Function**	On 15 July 2026, the Reserve Bank of India (RBI) initiated a consultation on the draft Guidance on Regulatory Expectations for Data Governance. The draft would apply to commercial banks (including foreign banks), small finance banks (SFBs), payments banks, local area banks, regional rural banks (RRBs), urban co-operative banks (UCBs), and rural co-operative banks (RCBs), All India Financial Institutions (AIFIs), non-banking financial companies (NBFCs) in all four layers, asset reconstruction companies and credit information companies. RBI stated that ongoing supervisory assessments continue to reveal data management weaknesses that pose operational, compliance, and financial risks. To address these gaps, the draft framework draws on local supervisory insights and international best practices, including the Basel Committee on Banking Supervision's principles for effective risk data aggregation and risk reporting (BCBS 239). Regulated entities would be expected to put in place a board-overseen data governance framework, aligned with their risk management framework, proportionate to their size and complexity, reviewed at least annually, and covering data from origination to deletion in compliance with the Digital Personal Data Protection Act, 2023 and its 2025 Rules. RBI's Directions would prevail in any inconsistency. Key proposals include: • A board-level data governance committee to oversee the framework and its policies, and an executive-level committee to implement and operationalise it; • A data function headed by an officer not below Chief General Manager rank or equivalent, with a data owner and data steward for each data domain and a data custodian for technical management; • A single source of truth for every data element, with no parallel or competing sources, designations approved by the executive committee and reconciliation with downstream data; • Metadata created at capture that flows with the data downstream, documented lineage and a classification framework reflecting the data's risk, criticality and sensitivity; • Data quality metrics and persistent issues reported to the board-level data governance committee at least quarterly; • Data shared with third parties, including group entities, only for approved purposes on a need-to-know basis, under non-disclosure clauses and subject to periodic audit; and • Periodic internal and external audits of the framework, including by Indian Computer Emergency Response Team-empanelled auditors where applicable, reported to the board's Audit Committee. RBI Consults on Data Governance Expectations Including a Single Source of Truth and a Senior Data Function | RBI	Public consultation ended on 17 August 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

India (2/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**RBI**	**RBI Consolidates Cybersecurity, Technology Risk and Digital Payment Security Requirements into Tiered Master Directions**	On 31 July 2026, RBI issued Cybersecurity, Technology: Risk, Resilience and Assurance Framework Directions and Digital Payment Security Controls Directions as part of its 64 Consolidated Supervisory Directions. The package carries forward existing supervisory instructions without substantive change. The cybersecurity Directions apply to commercial banks, SFBs, payments banks, UCBs, AIFIs, NBFCs, and credit information companies. The digital payment Directions apply to commercial banks, SFBs, payments banks, UCBs and credit card-issuing NBFCs. Both took effect immediately. Commercial banks, SFBs, AIFIs and credit information companies apply the cybersecurity framework in full. This includes: • board-level IT Strategy Committee (ITSC) of at least three directors, chaired by an independent director with seven years' IT experience and meeting quarterly; • Chief Information Security Officer who does not report to the head of IT; and • cyber security operations centre. Smaller entities are tiered. UCBs are assigned one of four levels by digital depth and interconnectedness, and only Level IV requires 24x7 security operations. NBFCs are tiered by regulatory layer: Base Layer NBFCs below INR 500 crore and Core Investment Companies follow the lightest chapter. Foreign bank branches may comply or explain on specified provisions. Key requirements carried forward include: • Cyber incidents reported on RBI's DAKSH platform within six hours of detection, with proactive notification to the Indian Computer Emergency Response Team (CERT-In); • Vulnerability assessment at least every six months and penetration testing at least annually for critical and internet-facing systems; • Disaster recovery drills at least half-yearly for critical systems, including operation from the recovery site for a full working day; • Multi-factor authentication for digital payments, with at least one dynamic or non-replicable factor; • Reconciliation of digital payment transactions within 24 hours of receipt of settlement files; • Device binding for mobile banking apps, with older app versions deactivated within six months of a new release; and • Payment Card Industry standards and hardware security module controls for card businesses, which apply to UCBs only at Level IV, or at Level III with assets of INR 5,000 crore and above. From 1 October 2026, commercial banks and SFBs may delegate the annual review of digital payment policies to the ITSC, with material amendments still requiring board approval. Reserve Bank of India issues Consolidated Supervisory Directions | RBI Reserve Bank of India (Commercial Banks – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026 | RBI Reserve Bank of India (Commercial Banks – Digital Payment Security Controls) Directions, 2026 | RBI	ITSC delegation for commercial banks and SFBs effective on 1 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Indonesia



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Indonesia (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	OJK	**OJK Issues Reporting Guidelines and Formats for Digital Financial Asset Trading Operators**	On 30 June 2026, the Otoritas Jasa Keuangan (OJK) issued Regulation of the Member of the Board of Commissioners (PADK) No. 3 of 2026 on the Operation of Digital Financial Asset Trading, including Crypto Assets. It implements OJK Regulation (POJK) No. 27 of 2024, as amended by POJK No. 23 of 2025, and sets reporting guidelines and formats for digital financial asset trading operators. These comprise exchanges, clearing, guarantee and settlement institutions, custodians, traders and other parties designated by OJK. The regulation prescribes: • Evaluation reports on the digital financial assets in OJK's official list of tradable digital financial assets; • Monthly, quarterly and annual periodic reports, including an annual activity report; • A risk management self-assessment report; • Incidental reports; and • Notifications by clearing, guarantee and settlement institutions on the clearing, guarantee and settlement of digital financial asset derivative transactions. The regulation replaces OJK Circular No. 20/SEOJK.07/2024 on digital financial asset trading in stages: • Specified reporting provisions and Attachment V are revoked from 1 July 2026; • Further provisions and part of Attachment VIII are revoked from 1 January 2027; and • The remainder is revoked on the regulation's effective date, except for the provisions preserved under Article 2. OJK Issues Reporting Guidelines and Formats for Digital Financial Asset Trading Operators | OJK	Effective on 1 September 2026; and Remaining provisions of SEOJK 20/SEOJK.07/2024 revoked in stages to 1 January 2027.
2	OJK	**OJK Brings Governance and Risk Management Requirements for Financial Sector Technology Innovation Providers into Force**	On 1 July 2026, POJK No. 30 of 2025 (POJK 30/2025) took effect, strengthening governance and risk management requirements for OJK-licensed Financial Sector Technology Innovation (ITSK) providers. These include providers of alternative credit scoring and of financial services aggregation. Licensed providers must establish governance and risk management arrangements under the regulation, including requirements relating to organisational responsibilities, risk management and reporting to OJK. The regulation is not a general artificial intelligence (AI) law and does not regulate AI providers or AI systems as a standalone category. OJK Brings Into Force Governance and Risk Management Obligations for Financial Sector Technology Innovation Organisers, Including AI and Digital Finance Platforms | OJK	Effective on 1 July 2026.

Indonesia (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	**Government of Indonesia**	**Indonesia Issues Implementing Regulation for the Personal Data Protection Law**	On 16 July 2026, Indonesia promulgated Government Regulation (PP) No. 33 of 2026 implementing the Personal Data Protection Law (Law No. 27 of 2022), effective 16 January 2027. The PP governs individuals, corporations, public bodies, and international organizations performing legal acts to protect personal data within Indonesia, or extraterritorially where actions impact Indonesia or offshore Indonesian citizens. Individual personal or household processing is excluded. Specific personal data includes personal financial data, elucidated as bank deposit balances and credit card data. Controllers must establish a lawful processing basis (e.g., explicit consent, contract performance, legal obligations, or legitimate interests) and notify data subjects—or do so within 30 working days for indirectly obtained data. Both controllers and processors must record processing, secure data based on risk, and supervise involved parties. Processors must follow controller instructions and obtain written approval to engage sub-processors. The personal data protection institution supervises compliance, issues written orders, and imposes administrative sanctions, coordinating with agencies like the OJK for financial controllers. Specified data subject rights and controller obligations are exempted only to implement a statute under prescribed criteria for national defense, law enforcement, public administration, or state supervision of financial, monetary, payment, and financial stability systems. Highlights of the regulation include: • **Data Subject Requests:** Within 72 hours of receiving a data subject's request, once verified, controllers must update or correct personal data, give access, stop processing after consent is withdrawn, and delay/ restrict processing; • **Automated Decisions:** Data subjects have the right to object to solely automated decisions, including profiling, with legal consequences or a significant impact, and controllers are required to have a response mechanism; • **Data Breach Notification Protocol:** Controllers must notify the affected data subject and the Lembaga in writing within 72 hours after becoming conclusively aware of a personal data protection failure. Public notification is also required where the failure disrupts public services or seriously affects the public interest, while processors must notify controllers of such failures at the earliest opportunity; • **Mandatory Data Protection Impact Assessments (DPIAs):** Controllers must conduct a data protection impact assessment before processing with potential high risk to data subjects, including automated decision-making with legal consequences or a significant impact, processing of specific personal data, large-scale processing, systematic evaluation, scoring or monitoring, and use of new technology; • **Appointment of Data Protection Officers (DPOs):** Controllers and processors must appoint a data protection officer where processing is for public services, or the controller's core activities require regular and systematic large-scale monitoring of personal data or consist of large-scale processing of specific or crime-related personal data; • **Cross-Border Transfer Requirements:** For transfers abroad, controllers must ensure the recipient's country offers protection at least equal to the Law's, or otherwise adequate and binding protection, and, failing both, must obtain the data subject's consent; • **Penalties and Administrative Fines:** Specified breaches attract, singly or together, a written warning, temporary suspension of processing, erasure or destruction of personal data or an administrative fine of up to 2% of the controller's or processor's annual revenue or receipts, applied against violation variables such as impact, duration and number of data subjects affected; and • **Transitional Provisions and Regulatory Continuity:** Existing laws and regulations on personal data protection remain in force where not in conflict with the PP, and, pending Lembaga regulations on processing, controllers and processors process on the same condition. Government of Indonesia Issues the Implementing Regulation for the Personal Data Protection Law | Government of Indonesia	Effective on 16 January 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Indonesia (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	**OJK**	**OJK Issues Rules on Reporting and Requests for Funding Transaction Data by Fintech Lending Operators**	On 5 August 2026, OJK announced the issuance of POJK No. 8 of 2026 on Reporting and Requests for Funding Transaction Data by operators of information technology-based joint funding services (LPBBTI), also known as Pindar. OJK stated that the regulation aims to improve the quality of funding transaction data, strengthen industry discipline, support risk-based supervision and strengthen the data infrastructure for digital financial services. Operators must submit funding transaction data to OJK through an OJK-managed reporting system, which OJK states is moving to a two-way structure. The data must be complete, accurate, current, intact and timely. Operators must also report to the industry association through the Fintech Data Center. The regulation sets a mechanism for requesting fund recipient information, which operators may use only for disbursement, risk management and compliance purposes set out in legislation. Key requirements include: • Each operator must appoint a member of its board of directors as responsible for transaction data reporting; • Operators must maintain written policies and procedures on data submission and on the use of fund recipient information; • Operators must conduct periodic internal audits of the reporting system and segregate duties in managing it; • Operators and associations are prohibited from providing or selling user information to third parties, except as required by law; and • OJK will impose administrative sanctions for breaches of the reporting, information-use or governance requirements. OJK Issues Rules on Reporting and Requests for Funding Transaction Data by Fintech Lending Operators | OJK	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Indonesia (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	OJK	**OJK Sets the Form and Content of Governance Reports for Financial Sector Technology Innovation Operators**	On 24 August 2026, OJK issued Regulation of the Member of the Board of Commissioners (PADK) No. 9 of 2026. It sets out a standard form and structure for the good governance reports that Financial Sector Technology Innovation (ITSK) operators must submit to OJK. The PADK implements Article 47(8) of OJK Regulation No. 30 of 2025 (POJK 30/2025) on governance and risk management for ITSK operators. The regulation is intended to support operators in applying good governance and to set out how, and when, they report on it. Each report must contain at least three parts: a transparency disclosure of how the operator applies good governance principles, a self-assessment of that implementation and, where weaknesses remain, an action plan. The action plan must set out the weaknesses, the corrective actions, target completion dates and any obstacles. The disclosure and the self-assessment both cover 11 aspects: • The duties and authority of shareholders and the general meeting of shareholders; • Active oversight by the board of directors and the board of commissioners; • Risk management; • Internal audit; • External audit; • Actual and potential conflicts of interest; • Information disclosure; • Business ethics; • The feasibility of the annual business plan; • Transparency of financial and non-financial condition; and • Controls over personal data protection and information system security. From the same date, OJK revoked Section II.E of Appendix II of OJK Circular Letter No. 4/SEOJK.07/2025 on reporting for ITSK, digital financial assets and crypto assets. Operators submit their first report in the new format for the December 2026 reporting position. PADK 9 Tahun 2026 Bentuk dan Susunan Laporan Penerapan Tata Kelola Yang Baik bagi Penyelenggara ITSK | OJK	Effective on 24 August 2026. First report covers the December 2026 reporting position and is due by 30 April 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	JFSA	**JFSA Adds Five Jurisdictions to the Travel Rule Designations for Crypto-Asset and Electronic Payment Instruments**	On 7 July 2026, the Financial Services Agency (JFSA) promulgated an amendment to the joint JFSA and Ministry of Finance (MOF) Notification No. 2 of 2023. This notification designates countries and regions under Articles 17-2 and 17-3 of the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds. The amendment adds Anguilla, Botswana, the Commonwealth of Dominica, Cuba and Oman to the list, increasing the number of designated jurisdictions from 58 to 63. The rule requires crypto-asset exchange service providers and electronic payment instrument service providers to notify originator and beneficiary information when transferring these assets. It applies to transfers to foreign service providers located in jurisdictions with regulations equivalent to Japan's. The JFSA identifies these jurisdictions by their implementation of the travel rule, referencing Financial Action Task Force (FATF) mutual evaluations, follow-up reports and local laws. JFSA Adds Five Jurisdictions to the Crypto-Asset Travel Rule Designation | JFSA	Effective on 3 August 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	JFSA	**JFSA Sets Phishing-Resistant Authentication and Anti-Phishing Expectations for Online Services of Insurers, Money Lenders and Payment Firms**	On 17 July 2026, the JFSA published the results of its public consultation and applied amendments to eight sets of supervisory and administrative guidelines, to strengthen the response to cyber risks that have increased in recent years. The amendments create dedicated sections on online (internet) transactions in the guidelines for insurance companies, small-amount and short-term insurance providers, money lenders, prepaid payment instrument issuers, and funds transfer service providers. They also extend related expectations to insurance brokers, financial services intermediaries and the electronic payment services of banks, building on the JFSA's Guidelines for Cybersecurity in the Financial Sector. Uniform implementation is not required, and each firm should assess its own risks. Where system development takes time, a phased rollout by customer segment is acceptable, although early implementation is encouraged. Firms are also expected to ensure that outsourced service providers implement equivalent fraud prevention measures. Key changes include: • **Phishing-resistant multi-factor authentication (MFA):** phishing-resistant MFA, such as passkeys or certificate-based log-in, is expected to be implemented and made mandatory by default for important operations such as logging in, withdrawing money and changing the account to which funds are paid. Until then, firms are expected to offer another multi-factor method and tell customers when the stronger method will arrive; • **Customer opt-out:** customers may switch this authentication off only where they cannot use it for unavoidable reasons, such as not having a suitable device. In that case, firms are expected to offer an alternative multi-factor method and monitor how many customers opt out; • **Access monitoring:** firms are expected to alert customers to log-ins, transactions and withdrawals they may not recognise, lock accounts after repeated failed log-in attempts, and analyse log-in behaviour to detect unauthorised access; • **Log-in links in communications:** emails and text messages are in principle not to contain links to log-in pages or pages asking for passwords unless there is no alternative. Firms are expected to adopt sender authentication technology and seek the takedown of phishing sites; • **Response and reporting:** firms are expected to respond sincerely to customers who suffer losses from fraudulent transactions, including through compensation, and to report unauthorised access or transactions to the authorities promptly in a crime occurrence report; and • **Intermediary security verification:** financial institutions partnering with financial services intermediaries are expected to verify that those intermediaries implement sufficient cybersecurity and anti-phishing measures. The intermediaries must themselves apply these measures directly where that better protects their customers. JFSA Sets Phishing-Resistant Authentication and Anti-Phishing Expectations for Online Services of Insurers, Money Lenders and Payment Firms | JFSA	Effective on 17 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	**Cabinet Office**	**Cabinet Office Publishes Draft Second Artificial Intelligence Basic Plan Centred on Agentic AI and AI Sovereignty**	On 14 July 2026, Japan's Cabinet adopted the Second Artificial Intelligence Basic Plan, succeeding the first AI Basic Plan adopted on 23 December 2025. The plan provides for revision, in principle annually, and sets out national policy priorities and planned government measures. The plan attributes the revision to AI's progression between late 2025 and mid-2026 from a tool supporting document preparation towards systems capable of making decisions and executing. Building on the first plan's support for AI agents and physical AI, it places greater emphasis on vertical AI and physical AI as Japan's route to AI Transformation (AX). It promotes open "AI sovereignty", aimed at avoiding excessive dependence on particular countries or companies while maintaining international cooperation and interoperability, and "responsible agile governance" to address increasingly complex risks. It retains the four strategic pillars: adopt AI, create AI, enhance AI trustworthiness, and collaborate with AI. Key priorities and planned measures include: • **Vertical and physical AI:** Promoting development, demonstration and implementation across fields including finance, healthcare, long-term care, education, policing, disaster risk reduction, manufacturing, infrastructure, logistics and telecommunications, including the active introduction of agentic AI. • **Project YATA-Shield:** Advancing cybersecurity measures through early initiatives in the financial sector and their extension to other sectors, alongside wider measures for government and critical infrastructure, with the Financial Services Agency among the responsible authorities. • **Personal information protection:** Preparing subordinate legislation and other measures to implement the amendments to the Act on the Protection of Personal Information, passed on 10 July 2026. These include a conditional consent exception for third-party provision of personal data used solely for qualifying statistical compilation, including qualifying AI development, and an administrative surcharge regime for specified violations. These provisions will apply following their commencement, subject to the statutory safeguards and implementing rules. • **AI Safety Institute:** Strengthening capabilities for model evaluation, traceability, guardrails and crisis-time information sharing, and establishing mechanisms to feed evaluation results into policies, guidelines and ministry operations. • **AI risk categories:** Highlighting technical risks, such as cascading failures caused by AI malfunctions; social risks, including unclear accountability and effects on work and employment; and national security risks, including autonomous AI-enabled cyberattacks. • **Responsible agile governance:** Combining institutional, technical and organisational-management measures, including controls and standards built into model design, improved AI literacy and clearer responsibilities. • **Human oversight and accountability:** Discussing human-in-the-loop, human-on-the-loop and human-in-the-lead approaches, while placing human agency, judgement and responsibility at the core of collaboration between people and AI. • **Government AI "Gennai" (源内):** Expanding the government's generative AI environment through a large-scale demonstration targeting approximately 180,000 staff. Parts of its software were released as open source in April 2026 to support adoption by local authorities and other organisations. • **International cooperation:** Seeking to host an AI Summit in Japan at an early date to advance international cooperation on trustworthy AI. Cabinet Office Publishes Draft Second Artificial Intelligence Basic Plan Centred on Agentic AI and AI Sovereignty | Cabinet Office	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	JFSA	**JFSA Moves Cyber-Incident Reporting onto Inter-Agency Common Forms Across the Supervised Population**	On 18 September 2026, JFSA published the results of its consultation on amendments to the Comprehensive Supervisory Guidelines for Major Banks, etc. and 16 other supervisory and administrative guidelines. The amendments reach banks, cooperative financial institutions, insurers, financial instruments business operators, money lenders, payment service providers, crypto-asset exchange service providers and other supervised entities. They follow the 15 September 2026 revision of the inter-ministerial agreement on reporting procedures when cyberattacks cause damage, which added a common form for other cyberattacks and system failures to the existing common forms for DDoS and ransomware attacks. Key changes include: • **Common forms:** system failures and cyber incidents are reported on the inter-agency common forms, replacing the JFSA's own system failure report forms; • **Timing:** institutions must continue to report immediately on becoming aware of an incident, report again on recovery and once the cause is identified, and give a status update within one month if recovery or cause identification remains outstanding; • **Personal data:** where personal data is leaked in connection with a ransomware incident or other cyberattack/system-failure incident, the common form may also be used for the personal data breach report; and • **Transition:** institutions other than operators designated by the JFSA Commissioner as specified critical infrastructure business under the Economic Security Promotion Act may keep using the existing JFSA system failure report form until the end of March 2027. The JFSA stated that the amendments mainly concern the move to the new forms and do not change the criteria for what must be reported. System failures not caused by a cyberattack are reported on the form for other cyberattacks and system failures, which also covers computer system failures, and no form needs to be chosen for the first immediate report. The JFSA said it will provide supplementary notes on reporting with the common forms. JFSA Moves Cyber-Incident Reporting onto Inter-Agency Common Forms Across the Supervised Population | JFSA	Public consultation ended on 7 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia (1/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	BNM	**Parliament Passes Cybercrime Bill 2026 Introducing an Offence for Distributing AI-Generated or Manipulated Content**	On 1 July 2026, the Dewan Rakyat passed the Cybercrime Bill 2026, and the Dewan Negara followed on 20 July 2026. The bill awaits royal assent and publication in the Gazette. It would consolidate Malaysia's cybercrime law into a single statute covering offences against computer systems and data, computer-related forgery and fraud, the national digital identity service, identity theft and synthetic content. It would also apply extraterritorially once in force. Clause 23 carries the synthetic media offence. It covers distributing, publishing, selling or making available visual or audio content that: • is generated or manipulated by a computer system; • resembles an existing person, object, place, entity or event; and • falsely appears authentic, where this is done with intent to commit or facilitate an offence under any written law. Conviction would carry a fine of up to RM 500,000, imprisonment of up to seven years, or both. Key proposals include: • Clause 22 would create an identity theft offence, and clause 17 a computer-related fraud offence; • Clause 24 would penalise distribution of intimate images, whether altered or not, with up to five years' imprisonment or a fine of up to RM 300,000. This would rise to seven years or RM 500,000 where done with intent to shame, harm, coerce or threaten the person depicted; • Clause 25 would apply strengthened penalties where an offence under Part III or IV, or clauses 21, 22 or 23, affects or involves a national critical information infrastructure entity; • Clause 19 would penalise disclosing a national digital identity service password with a fine of up to RM 100,000 or imprisonment of up to three years, with a rebuttable presumption where disclosure was made for gain; and • Part II would establish a Committee to Combat Cybercrime with power to establish subcommittees and invite others to attend. Parliament Passes Cybercrime Bill 2026 Introducing an Offence for Distributing AI-Generated or Manipulated Content | Parliament	Passed by the Dewan Rakyat on 1 July 2026 and the Dewan Negara on 20 July 2026. Awaiting royal assent and gazettal.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia (2/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**BNM**	**BNM Invites Applications for Financial Technology Regulatory Sandbox Green Lane Cohort**	On 1 July 2026, BNM announced an open application window for the Financial Technology Regulatory Sandbox Green Lane cohort to accept submissions from 1 to 31 July 2026. The Green Lane provides licensed financial institutions, including banks, development financial institutions, insurers, takaful operators, and money services businesses, with an accelerated pathway to test innovative solutions facing regulatory impediments, through a one-off institutional risk assessment and simplified solution-level registration process. Eligible applicants must submit a list of proposed solutions with descriptions, target segments, and regulatory impediments identified, together with an aggregate cap assessment on expected financial losses attested by the CEO and Chief Risk Officer. Testing within the Green Lane is limited to 20,000 unique customers per registered solution over a maximum 12-month period. Non-financial institutions may participate only through collaboration with an eligible Green Lane participating institution. BNM Invites Applications for Financial Technology Regulatory Sandbox Green Lane Cohort | BNM BNM Financial Technology Regulatory Sandbox Green Lane Application Form | BNM BNM Financial Technology Regulatory Sandbox Policy Document | BNM BNM Financial Technology Regulatory Sandbox Website | BNM	Deadline for full phase-out of proprietary QR code scheme networks: 30 June 2028.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia (3/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	SC	**SC Consults on a Proposal to Strengthen Technology and AI Corporate Governance**	On 3 July 2026, the Securities Commission Malaysia (SC) consulted on *Proposals to Strengthen Corporate Governance Ecosystem,* including proposed technology governance and disclosure expectations for public listed companies (PLCs). The proposals would inform the upcoming Malaysian Code on Corporate Governance (MCCG) 2026. Technology governance was one of four key topics covered, encompassing artificial intelligence (AI), digitalisation, cybersecurity, data-driven tools and automation. The proposals emphasise board oversight of both technology-related risks and opportunities for innovation and long-term value creation. **Core Board Expectations** Under the proposals, boards of PLCs would be expected to: • **Oversee Strategy and Resources:** Align technology adoption with long-term value creation, ensuring adequate talent, investment and resource allocation, while considering opportunities to improve productivity, efficiency, innovation and competitiveness. • **Manage Technology Risks:** Oversee cybersecurity, data governance, privacy, model risks and overall operational resilience. • **Maintain Human Oversight and Escalation:** Ensure mechanisms are in place to monitor, escalate and address technology and AI incidents, and maintain appropriate human oversight of technology and AI-enabled decisions and outcomes, where relevant. • **Strengthen Governance, Accountability and Capability:** Establish clear technology governance structures, maintain accountability for technology-related decisions and outcomes, and ensure the board and management maintain sufficient collective technology literacy. **Proportionate Disclosure Framework** To improve transparency, the SC proposes that PLCs disclose their technology adoption philosophy, governance structures, risk management processes and methods for maintaining board and management technology literacy, competency and access to relevant expertise. Disclosures would also cover how technology supports business strategy and operational objectives, incident monitoring and escalation mechanisms, and measures for maintaining appropriate human oversight where relevant. The proposed disclosures should be meaningful, company-specific and proportionate to a PLC's strategy, business model, size, complexity, digital dependency and risk profile. Companies should avoid boilerplate language, while ensuring published information does not compromise cybersecurity, commercial sensitivity or confidentiality. SC Seeks Public Feedback on Key Proposals to Strengthen Corporate Governance Ecosystem - Media Releases | Securities Commission Malaysia	Public consultation ended on 31 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia (4/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	NAIO	**NAIO Consults on Proposed AI Governance Bill Introducing a Central AI Authority, Tiered Risk Framework, and Incident Reporting**	On 10 July 2026, Malaysia's National AI Office (NAIO) published the AI Governance Bill Public Consultation Paper, marking a pivotal transition from voluntary ethical guidelines to Malaysia's first legally binding statutory framework for artificial intelligence. Based on the Public Consultation Paper, the proposed Bill introduces a three-pronged regulatory approach. It combines central institutional oversight leveraging existing sectoral expertise with a principle-based national baseline for responsible AI lifecycle management, alongside a risk-based framework ensuring regulatory obligations remain strictly proportionate to each system's nature, context, and risk level. The paper sought preliminary feedback across six proposed areas of the legislation: scope, AI governance architecture, AI governance principles, the AI risk framework, AI incident reporting, and an AI sandbox. Regardless of hosting location, the proposed framework applies to AI systems developed, marketed, or used in Malaysia—or by a Malaysia-established deployer—except for those used strictly for personal affairs, national defense, or security. The Bill proposes a Central AI Authority exercising AI safety, investigation and enforcement, and AI enablement functions, with Sectoral Leads able to be appointed and delegated specific powers to translate the national framework into sectoral instruments. Five AI Governance Principles—human dignity and agency, transparency and explainability proportionate to risk and impact, accountability through traceability and effective redress, safe and secure use through robust and resilient systems, and responsible data governance and stewardship—would impose a "due regard" duty on Developers and Deployers throughout the AI lifecycle, with accountability allocated according to each party's degree of control at the relevant stage. The proposed risk framework is anchored to four baseline harm categories, namely death, bodily injury, unlawful deprivation of fundamental liberty under the Federal Constitution, and contravention of any written law, evaluated by likelihood, severity and scale, and duration and reversibility, then sorted into three tiers. Three tiers of risk are defined as: • **Tier 1 (Unacceptable):** Any AI system developed or deployed with the intent to cause the defined harms; • **Tier 2 (High Risk):** Systems developed or deployed without intent to cause harm but creating a risk of harm, potentially subject to risk assessment, documentation, internal controls, human oversight, monitoring and mitigation measures; and • **Tier 3 (Low Risk):** Systems showing no foreseeable material AI harm, subject only to baseline due regard for the principles and lighter compliance approaches. Under the current proposal, a reporting requirement would apply to all "AI incidents," defined broadly as any failure, weakness, misuse, unexpected effect, or near-miss event that causes or has the potential to cause AI-related harm. Implementation would be phased, with voluntary instruments issued in the initial stages and codification of the principles considered once ecosystem maturity is reached. Requirements may be issued by class of AI System (Developer as primary duty holder), by sector through designated Sectoral Leads, or by domain of deployment (Deployer as primary duty holder). NAIO Consults on Proposed AI Governance Bill Introducing a Central AI Authority, Tiered Risk Framework, and Incident Reporting | NAIO	**Public consultation ended on 31 July 2026.**

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia (5/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	**JPDP**	**JPDP Consults on an AI Framework Applying Personal Data Protection Act Obligations Across the AI Lifecycle**	On 5 October 2026, the *Jabatan Perlindungan Data Peribadi* (JPDP) initiated a consultation on a proposed Framework for AI and Personal Data Protection. The framework would be issued as guidelines under subsection 48(g) of the Personal Data Protection Act 2010 (Act 709), and would apply to data controllers, data processors, and third-party service providers and AI vendors processing personal data through AI systems, whether developed in-house, procured, customised, or embedded in platforms delivered as software-as-a-service or through application programming interfaces. JPDP highlights that the use of an AI system would not create a separate legal basis for processing. All data processing through an AI system, including the collection of personal data for development, training, testing, and validation, would remain subject to Act 709. The proposed framework covers ten parts across the entire AI lifecycle, from legal basis and development through deployment, acquisition of external AI, data subject rights, safeguards and fairness, governance and risk management, and documentation and audit. Key proposals include: • **Data protection impact assessments** would be conducted where appropriate, addressing data type, volume, and sensitivity, the AI system's purpose and complexity, the risk of inaccurate, biased or discriminatory outputs, and the severity of decision-making impact; • **Written notice to data subjects** would state whether an AI system makes or supports decisions affecting them or produces recommendations or predictions, with a new or amended notice required when the processing purpose differs materially; • **Anonymised or pseudonymised data** would be preferred where development, training, testing, or validation can reasonably be achieved without directly identifying data subjects; • **Personal data** could not be retained solely because it had been used by or associated with a decommissioned AI system, and would be securely deleted, anonymised, or disposed of once no longer needed; • **Due Diligence** on external AI would address whether personal data is stored, reused or used for model training, fine-tuning, optimisation or analytics beyond the intended service, with controllers able to request model cards, system cards, or technical documentation; • **Cross-border transfers** would require compliance with section 129 of Act 709 and a Transfer Impact Assessment under the Commissioner's Cross-Border Transfer Guidelines; • **Material modification, retraining, or updating after deployment** would trigger reassessment, testing, or validation before the changed system is used; and • **Documentation across the AI system lifecycle** would be maintained and submitted to the Commissioner on request. JPDP Consults on an AI Framework Applying Personal Data Protection Act Obligations Across the AI Lifecycle | JPDP	Public consultation ends on 23 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

New Zealand



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

New Zealand (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**OPC**	**OPC Biometric Processing Privacy Code Takes Full Effect as the Transition Period for Existing Users Ends**	On 3 August 2026, the nine-month transition period under the Biometric Processing Privacy Code 2025 ended for agencies that were already using biometric processing when the Code came into force on 3 November 2025. The Office of the Privacy Commissioner's (OPC) Code now applies in full, with no further transitional relief, to organisations and businesses that collect and use biometric information. This covers physical or behavioural features such as faces, fingerprints, voices, keystroke patterns or gait. Amendment No. 1 to the Code, issued in March 2026 to reflect the new Information Privacy Principle 3A, has been in force since 1 May 2026. The OPC has published detailed guidance, use case examples and six summary factsheets covering: • an overview of the Code; • collection; • use; • disclosure; • access and correction requests; and • storage, security, retention and disposal. OPC Biometric Processing Privacy Code Takes Full Effect as the Transition Period for Existing Users Ends | OPC	Code applies in full to existing biometric processing from 3 August 2026.
2	**Standards New Zealand**	**Standard New Zealand Consults on Adopting 14 International AI Standards as New Zealand AI Standards**	On 14 August 2026, Standards New Zealand initiated a consultation on the ITSP P5002D collection of 14 international AI standards proposed for adoption as New Zealand standards under draft DZ NZS ISO/IEC designations. The collection is one of five under the International Technology Standards Programme (ITSP), which the Department of the Prime Minister and Cabinet commissioned so that New Zealand keeps pace with global developments and shapes the standards underpinning emerging technologies. Standards New Zealand described the standards as internationally recognised guidance for the responsible development, deployment, governance, and use of AI system. The standards proposed for adoption cover: • **Governance and Assurance:** ISO/IEC 38507 on the governance implications of AI use by organisations, ISO/IEC 42005 on AI system impact assessment, and ISO/IEC 42006 on requirements for bodies auditing and certifying AI management systems; • **Transparency and Fairness:** ISO/IEC 12792 on a transparency taxonomy for AI systems, ISO/IEC TS 6254 on explainability and interpretability, and ISO/IEC TS 12791 on treating unwanted bias in machine learning; • **Data Quality:** Three parts of ISO/IEC 5259 on data quality for analytics and machine learning, including data quality measures and a data quality governance framework; • **Testing and Sustainability:** ISO/IEC TS 42119-2 on testing AI systems and ISO/IEC TR 20226 on the environmental sustainability of AI systems; and • **Big Data:** ISO/IEC 20546 on big data vocabulary and two parts of the ISO/IEC 20547 big data reference architecture. Standards New Zealand stated that adopting international standards improves alignment with globally recognised good practice, enhancing quality, safety and reliability, and supports market access through a common technical framework. Five review committees are assessing the ITSP collections, and the public is invited to comment on whether the standards should be adopted, particularly any reasons for not adopting them. Standard New Zealand Consults on Adopting 14 International AI Standards as New Zealand AI Standards | Standard New Zealand	Public consultation ended on 8 October 2026.

Philippines



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	BSP	**BSP Publishes the Project Agila Report Identifying Securities Settlement and Cross-Border Payments as Wholesale CBDC Use Cases**	On 1 July 2026, BSP published its Project Agila report, setting out the results of its wholesale central bank digital currency (wCBDC) project with six financial institutions: BDO Unibank, China Banking Corporation, Land Bank of the Philippines, Rizal Commercial Banking Corporation, Union Bank of the Philippines and Maya Philippines. A wCBDC is a digital form of central bank money used for transfers between financial institutions rather than by the public. The project tested whether distributed ledger and tokenisation technology could let institutions transfer central bank money outside business hours, including when PhilPaSS Plus, the BSP's real-time gross settlement system, is unavailable. After a platform selection phase in 2023, proof-of-concept tests ran from April to September 2024 on Oracle's Hyperledger Fabric platform. Key findings include: • Transfers between institutions worked round the clock and were final once validated, with the platform processing up to 105,000 transactions a day, compared with an average of 6,789 a day on PhilPaSS Plus in the first quarter of 2025; • Performance weakened above 200,000 daily transactions, and confirmation speed, finality notifications, user onboarding and security controls such as multi-factor authentication need improvement; • Participating institutions saw liquidity management benefits from real-time settlement, automation and programmability, and the BSP sees a wCBDC as a potential back-up facility for PhilPaSS Plus; • A live wCBDC would likely be a systemically important payment system, and the report recommends clear access criteria, holding limits, no interest payments and treatment as a reserve instrument and high-quality liquid asset; and • The BSP's charter does not cover digital currency in its definitions of currency and legal tender, so the report suggests amendments or new legislation, although the National Payment Systems Act could support issuance. The project team recommended focusing next on the settlement of tokenised financial securities and institutional cross-border payments. The BSP will prepare a CBDC strategic roadmap setting out initiatives, timelines and success measures for each use case, and will continue working with supervised institutions, market infrastructures, government agencies and foreign central banks. BSP Publishes the Project Agila Report Identifying Securities Settlement and Cross-Border Payments as Wholesale CBDC Use Cases | BSP	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (2/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**Senate of the Philippines**	**Senate Bill Proposes an Artificial Intelligence Regulation Act with Mandatory Registration and a National AI Commission**	On 2 July 2025, Senator Pia S. Cayetano filed Senate Bill No. 25 in the 20th Congress to propose the Artificial Intelligence Regulation Act (AIRA). The bill would regulate the development and use of all types of artificial intelligence (AI), including foundation models, generative AI and large language models. It would apply to every individual, company, institution and government agency that develops, deploys, uses or operates AI systems in the Philippines. The explanatory note cites the European Union's AI Act and risks such as algorithmic bias, discrimination and AI hallucinations, where systems confidently produce false outputs. The bill would establish a National AI Commission (NAIC), attached to the Department of Science and Technology (DOST) and chaired by its Secretary. The NAIC would have original and exclusive jurisdiction over AI matters, with quasi-judicial powers to hear cases and impose sanctions. Ethical and sustainability reviews of AI systems would be carried out in coordination with sector regulators. Key proposals include: • **No AI system could be imported, sold, deployed or made publicly accessible without prior registration** with the NAIC. Registration would be a prerequisite for any business licence, and systems already in use would have to register within 60 days of the law taking effect; • AI **systems would be classified as high, moderate or low risk**. High-risk systems, including those used in finance, would require algorithmic impact assessments, data privacy reviews and sustainability screening before certification; • **Developers, deployers and operators would have to audit their systems** for bias, security and privacy, tell users when they are interacting with AI, and take full responsibility for harms; • They would also need a mechanism to immediately halt or disable a system that behaves unpredictably or exceeds its intended function; • **Employers adopting AI that may displace workers** would submit an AI Deployment Impact Report and notify the Department of Labor and Employment at least 60 days before implementation; and • **Penalties** would include fines of PHP 500,000 to PHP 5 million, or imprisonment of six months to three years, for deploying unregistered systems. Using AI to commit fraud or cause harm would carry fines of PHP 2 million to PHP 10 million, or six to twelve years' imprisonment. Senate Bill Proposes an Artificial Intelligence Regulation Act with Mandatory Registration and a National AI Commission | Senate of the Philippines	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (3/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	BSP	**BSP Issues Six Recommendations for Managing Emerging Risks Arising from Frontier AI Systems**	On 6 July 2026, the Bangko Sentral ng Pilipinas (BSP) issued Memorandum No. M-2026-034 to all BSP-supervised financial institutions, setting out six recommendations for managing cybersecurity risks from frontier artificial intelligence (AI) systems. The BSP describes these systems as able to find software weaknesses, build ways to exploit them and run multi-stage cyberattacks with little human involvement. It warns that the same capabilities could be turned against financial institutions, their third-party service providers and critical infrastructure. The recommendations build on the information technology and cybersecurity risk management rules that already apply to banks and non-bank financial institutions under the BSP's regulatory manuals. The memorandum closes by recommending that institutions formally establish an AI governance framework proportionate to the scale and materiality of their AI use, following the AI governance principles the BSP issued in June 2026. Key recommendations include: • **Keeping accurate, current inventories** of internet-facing assets, cloud services, user identities, critical applications and software components, including third-party and open-source components; • **Strengthening basic controls** through good credential management, multi-factor authentication for critical systems, minimum necessary access rights and hardened devices; • **Reducing exposure to attack** through network segmentation, zero trust controls, faster patching and the replacement of outdated platforms; • **Moving to phishing-resistant authentication**, such as hardware security keys or smart cards, and ending the use of passwords, SMS codes and push notifications for all administrative and privileged access; • **Using AI-enabled tools** for patching, threat hunting and security operations, with temporary "virtual patches" to block attacks before software updates are applied; and • **Updating business continuity plans** to prepare for AI-enabled attacks. BSP Issues Six Recommendations for Managing Emerging Risks Arising from Frontier AI Systems | BSP	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (4/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	BSP	**BSP Issues Voluntary AI Governance Principles Extending to Outsourced Service Providers**	On 24 June 2026, BSP announced its guidance paper, Governance Principles for Artificial Intelligence (AI) in Financial Services, issued to all BSP-supervised financial institutions under Memorandum No. M-2026-031. The principles also reach the vendors and outsourced service providers that support institutions' AI activities, under a shared-responsibility model in which each party answers for what it controls. Collectively known as the 'STARS' framework, the paper sets out five principles and maps risks and controls throughout the lifecycle of an AI system, spanning across planning, development, validation, deployment, and monitoring. Validation is to be carried out by a team independent of the developers. Compliance is voluntary, but the BSP described the principles as its minimum supervisory expectations for AI adoption. The BSP stated that fairness in algorithms and model risk will be addressed in a forthcoming model risk management framework, while other emerging technology risks remain under its existing information technology risk management rules. The five principles are: • **Sustainability:** attention to energy use, electronic waste and human-centred design, and building staff skills; • **Transparency:** a central inventory of AI systems, telling users when AI output is used, and documenting design, decisions and data sources so that systems can be audited; • **Accountability:** human oversight at every stage, clear ownership, competent leadership of AI development and the ability of the BSP to review AI algorithms; • **Responsibility:** well-prepared and representative training data, avoiding harm to minority or vulnerable groups, and clear opt-in and opt-out choices; and • **Security:** regular risk assessment, defences against attacks designed to manipulate AI systems or corrupt their data, and monitoring for bias and inaccurate outputs. BSP Issues Voluntary AI Governance Principles Extending to Outsourced Service Providers | BSP	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (5/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	**BSP**	**BSP Imposes Digital Bank Prudential Standards on Thrift, Rural and Cooperative Banks Operating Technology-Driven Models**	On 3 September 2026, BSP approved Circular No. 1240, amending the Manual of Regulations for Banks to set additional prudential requirements for thrift, rural and cooperative banks with technology-driven business models. The BSP stated that the measures aim to support prudent digital transformation while keeping these banks' operations aligned with their mandates and business models. Existing banks found to operate like a digital bank must meet digital bank requirements, including the same minimum capital, within six months of receiving BSP notice. Key changes include: • The BSP will impose **additional requirements where a bank operates like a digital bank**, or where its risk management and capital no longer match its business model and risk profile; • Additional requirements also apply to banks using digital platforms whose loans or deposits grow by more than 30% a quarter for two consecutive quarters; • **Measures may include extra capital** to meet the digital bank minimum, limits on activities or new digital products, enhanced supervisory reporting, and automated anti-money laundering and real-time fraud monitoring systems; • **Acquisitions intended to turn a bank into a technology-driven business must meet digital bank standards**, including the PHP 1.0 billion minimum capital; • The BSP may grant additional digital bank licences, including by converting existing thrift, rural and cooperative banks; and • Digital banks may open physical, non-transactional touch points, with the activities conducted there approved by the BSP. BSP Imposes Digital Bank Prudential Standards on Thrift, Rural and Cooperative Banks Operating Technology-Driven Models | BSP	Effective on 6 Oct 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	MAS	**MAS Sets Out AML/CFT Supervisory Expectations for Digital Payment Token Services Providers**	On 13 July 2026, the Monetary Authority of Singapore (MAS) published an information paper setting out its observations and supervisory expectations for digital payment token service providers' (DPTSPs) anti-money laundering, countering the financing of terrorism, and countering proliferation financing (AML/CFT/CPF) controls. Drawing on MAS inspections and ongoing engagements with licence applicants and licensees, the paper covers seven areas: new product and digital payment token (DPT) listing risk assessment, enhanced customer due diligence for higher-risk customers, value transfer requirements, ongoing monitoring, screening, partner and outsourcing due diligence, and training and staff expertise. The paper supplements MAS Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service and its accompanying Guidelines. Pre-listing DPT assessments should consider risks directly associated with the token, its track record and governance, market and economic indicators relating to manipulation and fraud, and smart contract and blockchain vulnerabilities, with ongoing adverse news monitoring formalised and documented. MAS expects DPTSPs to conduct a gap analysis of their existing frameworks and controls against the practices and supervisory expectations in the paper, taking into account their enterprise-level risk profile, with Board and senior management oversight of the assessment, root cause analysis, and timely remediation. Key requirements include: • **Documentation of Listing Deviations and Approvals:** Deviations from DPT listing policies, including cases where DPTs do not meet the DPTSP's risk appetite, should be documented with justifications, appropriate compliance or control function sign-off on the risk assessment and properly documented senior management approval; • **Assessment Thresholds and Criteria:** The reasons supporting DPT assessment thresholds and criteria, such as minimum market capitalisation and average daily traded volume, should be documented to facilitate periodic review and provide clarity on the risks to be mitigated; • **Enhanced Monitoring of Higher-Risk Customers:** Higher-risk customers are subject to enhanced monitoring through more frequent periodic reviews and/or enhanced transaction-monitoring rules; • **Source of Funds/Wealth Corroboration:** For source-of-funds assessments where incoming funds are DPTs, insights from blockchain analytics and/or other surveillance tools should augment or complement off-chain information. Where a customer's source of wealth is derived from virtual-asset activities, DPTSPs should understand the customer's virtual-asset exposure and obtain relevant supporting documents to corroborate the customer's virtual-asset transactions and holdings; • **Integration of Risk Frameworks and Indicators:** Customer risk frameworks should adequately consider on-chain and off-chain risk information and clearly set out the approach and risk indicators used to identify politically exposed persons and higher-risk customers, including the assessment of jurisdiction risks; • **Tailored and Role-Specific Training Programs:** Training should be tailored to staff members' functions, responsibilities and experience. Staff should be minimally equipped with a baseline understanding of blockchain technology, cryptocurrencies, the ML/TF risks arising from the DPTSP's products and services, and associated regulatory developments; and • **Committee Governance and Representation:** Relevant committees overseeing decision-making for key frameworks and controls should have balanced representation of technical DPT, AML/CFT and compliance expertise. MAS Sets Out AML/CFT Supervisory Expectations for Digital Payment Token Services Providers | MAS	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**PDPC**	**PDPC Finalises Advisory Guidelines on the Use of Personal Data in Generative AI**	On 20 July 2026, the Personal Data Protection Commission (PDPC) issued its finalised Advisory Guidelines on Use of Personal Data in Generative AI, together with its Response to Feedback. The Guidelines clarify how the Personal Data Protection Act 2012 (PDPA) applies across the development, deployment and post-deployment stages of the generative AI lifecycle. They follow a public consultation held from 2 June to 1 July 2026, which received responses from 40 organisations and three individuals. Against the draft, the final Guidelines remove the proposed best practice of notifying organisations controlling online data before web-scraping. Where it is reasonably arguable that personal data behind a digital barrier is not publicly available, but an organisation nevertheless relies on the Publicly Available Exception, it must document its assessment and reasoning in a Data Protection Impact Assessment or other written record, producible to PDPC on request. The Guidelines are advisory and not legally binding, with the PDPA and its subsidiary legislation prevailing in the event of any inconsistency. Key highlights include: • **Broadened Definition of Digital Barriers:** Expanding examples of digital barriers to include paywalls and subscriptions, registration requirements, authentication mechanisms, location or eligibility-based controls, and tools that restrict automated access. • **Consent Requirements:** Clarifying that the Consent and Notification Obligations apply only where deemed consent and exceptions to consent, including the business improvement and research exceptions, are unavailable. • **AI-Specific Notifications:** Confirming that AI-Specific Notifications are a shorthand for providing sufficient information to enable meaningful consent, rather than a prescribed template. Organisations may use existing privacy policies or terms of use, provided individuals can understand what User Data is used and how they are used. • **Definition of Model Development:** Defining "training" and "fine-tuning" as activities that develop or modify a model's parameters or underlying capabilities, excluding inference and operational activities such as Retrieval-Augmented Generation (RAG). • **Role-Based Controls:** Requiring stakeholders performing multiple roles such as Model Provider, System Provider and System Deployer to maintain policies and practices addressing the obligations applicable to each role. The Guidelines also identify information that Model and System Providers are encouraged to share with downstream stakeholders. • **Digital Barriers:** Encouraging organisations and individuals to implement appropriate digital barriers where they do not intend, or have not obtained consent, for personal data made available online to be web-scraped. • **Agentic AI Risks:** Acknowledging data-protection risks associated with agentic functionalities, while deferring comprehensive treatment of emerging agent-specific issues for separate study and guidance. • **Access and Correction Rights:** Clarifying that the Access and Correction Obligations apply to personal data collected, used or disclosed for model or system development or deployment. PDPC Finalises Advisory Guidelines on Use of Personal Data in Generative AI |PDPC Public Consultation on Proposed Advisory Guidelines on the Use of Personal Data in Generative AI | PDPC Response to Feedback on Public Consultation on Proposed Advisory Guidelines on Use of Personal Data in Generative AI | PDPC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	MAS	**MAS Managing Director Sets Out Operational, AI and Quantum Resilience Priorities at the MAS Annual Report 2025/2026 Media Conference**	On 28 July 2026, Mr Chia Der Jiun, Managing Director of MAS, delivered remarks at the MAS Annual Report 2025/2026 Media Conference. He outlined MAS' regulatory and supervisory priorities on operational resilience, technology and third-party risk, AI-enabled scams and cyber threats, and quantum resilience. Key regulatory developments include: • **Operational and technology resilience:** MAS referred to its March 2026 consultations on updated Guidelines on Operational Risk Management and Third-Party Risk Management, and to its ongoing consultation on amendments to the MAS Notices on Technology Risk Management. The proposed Notices cover IT asset management, IT capacity planning, continuous system and security monitoring, and data backup and recovery; • **AI-enabled scam detection:** MAS will review banks' efforts to improve their fraud-detection models, including their use of AI. MAS, GovTech, the Singapore Police Force and five banks are also testing whether AI models trained on cross-bank and public-private data can improve detection of scam transactions, with findings expected in 2027; • **AI-enabled cyber threats:** from 1 July 2026, MAS requires key financial institutions to conduct AI-assisted red teaming on critical internet-facing systems. MAS will also issue supervisory expectations for key financial institutions to submit assessments and action plans on vulnerability detection and patching, system-change testing, and the backup, restoration and recovery of critical systems and services. MAS announced the public-private AI-Driven Cyber and Tech Risk Taskforce (ABS-ACT) to coordinate this effort; and • **Quantum resilience:** MAS will issue supervisory expectations later in 2026 setting milestones and timelines for financial institutions to inventorise cryptographic assets, prioritise migration of vulnerable assets, and establish the capabilities and governance needed for quantum-safe migration. MAS aims for financial institutions to achieve quantum resilience before the end of 2029. Remarks by Mr Chia Der Jiun, Managing Director, MAS, at the MAS Annual Report 2025/2026 Media Conference on 28 July 2026 | MAS	AI-assisted red teaming required from 1 July 2026; Quantum supervisory expectations to be issued later in 2026; and Quantum resilience targeted before the end of 2029.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	MAS	**MAS Consults on Legislative Amendments to Implement Stablecoin Regulatory Framework**	On 1 September 2026, MAS initiated a consultation on proposed amendments to the Payment Services Act 2019 to introduce the regulatory framework for stablecoins in Singapore. The MAS Single-Currency Stablecoin (MAS-SCS) framework would cover single single-currency stablecoins issued in Singapore and pegged to the Singapore Dollar or any G10 currency. Only a licensed issuer could describe its token as an "MAS-regulated stablecoin", and stablecoins that are not MAS-regulated stablecoins would generally remain within the digital payment token regime. Key proposed requirements include: • A new stablecoin issuance licence would sit alongside the existing money-changing, standard payment institution, and major payment institution licences; • An issuer would generally have to incorporated in Singapore and would not be permitted to carry on any business other than issuing MAS-regulated stablecoins, except DPT services incidental to its own MAS-regulated stablecoins or other business prescribed or approved by MAS; • Issuers would be prohibited from paying holders interest, return, or any other benefit directly or indirectly attributable to holding MAS-regulated stablecoins, although this would not apply to revenue-sharing, distribution, service, or other commercial arrangements between an issuer and a third party; • Reserve assets would be held in a separate pool for each type of stablecoin, at not less than 100% of the par value in circulation, with composition, valuation, segregation, custody and insolvency safeguarding to be prescribed by regulations; • Holders would have a right to redeem at par in the pegged with the request fulfilled within a timeframe to be prescribed; • An auditor appointed at the issuer's expense would carry out a reserve asset attestation at a frequency MAS specifies, with the report submitted to MAS and published on the issuer's website; • Issuers would conduct regular stress testing against idiosyncratic and systemic shocks, with scenarios and results reviewed at board level and shared with MAS, and would maintain recovery and orderly wind-down plans. MAS proposes that the stress testing be conducted at least quarterly. Issuers would also maintain recovery and orderly wind-down plans; • Customer monies received before stablecoins are issued or paid following direct redemption requests would have to be safeguarded from the time they are received or become payable, as applicable; • **Banks and merchant banks wishing to issue MAS-regulated stablecoins would have to do so through a separate non-bank legal entity;** • Stablecoins jointly issued by a Singapore and one or more foreign issuers could be regulated under the framework and carry the MAS-regulated label, subject to case-by-case exemptions and safeguards concerning the foreign regulatory regime, supervisory cooperation, reserve assets, issuance and redemption terms, and recovery and orderly wind-up arrangements; • A limited number of foreign-issued stablecoins regulated under a foreign framework assessed to be substantively equivalent to the MAS-SCS framework could be recognised, subject to MAS being satisfied that they are well-regulated for value stability on an ongoing basis and that appropriate supervisory cooperation and information-sharing arrangements are in place; and • Issuers would be required to have the technical capability to trace, freeze, and/or burn their stablecoins where used for illicit activity, with specifics to follow by MAS notice. MAS Consults on Legislative Amendments to Implement Stablecoin Regulatory Framework | MAS Consultation Paper on Proposed Amendments to the Payment Services Act 2019 for Stablecoins Regulation | MAS	Public consultation ends on 16 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China)



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (1/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**Executive Yuan**	**Taiwan Promulgates the Virtual Asset Services Act Establishing a Licensing Regime for Virtual Asset Service Providers**	On 30 June 2026, Taiwan's Legislative Yuan passed the Virtual Asset Services Act. According to the FSC, the Act aims to promote the sound development and operation of virtual asset businesses, regulate virtual asset services and trading markets, protect traders' rights and interests, and foster financial innovation. Key points include: • **Comprehensive Regulatory Framework for VASPs:** The Act establishes a regulatory framework for seven categories of VASP activities, including exchange, trading platform, transfer, custody, underwriting, lending and other services, with requirements covering operational management, personnel fitness and propriety, internal controls, information security, customer asset protection and financial reporting; • **Stablecoin Issuance and Management Regime:** The issuance of stablecoins in Taiwan will require the consent of the Central Bank and approval from the FSC. Issuers must maintain full reserve assets, place assets in trust and comply with disclosure requirements; • **Enhanced Market Integrity and Trader Protection:** The Act prohibits fraudulent, deceptive and price manipulation activities. Violations may result in imprisonment of three to ten years and fines ranging from NTD 10 million to NTD 200 million; and • **Transitional Arrangements for Existing Operators:** Existing AML-registered VASPs and financial institutions already providing relevant services must apply for FSC permission within 12 months after commencement and obtain the required approval and licence within 21 months, subject to a one-time extension of up to three months. Regarding to the transition to comprehensive supervision and next steps, the FSC stated that VASP supervision will evolve from an AML-focused framework to a broader regime covering sound operations and market order. The FSC will continue drafting implementing regulations and consulting relevant stakeholders. Taiwan Promulgates the Virtual Asset Services Act Establishing a Licensing Regime for Virtual Asset Service Providers | Executive Yuan	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (2/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**MODA**	**MODA Issues AI Risk Classification Framework Setting Twenty Risk Sub-Types and a Four-Step Process for Competent Authorities**	On 7 July 2026, the Ministry of Digital Affairs (MODA) issued version 1.0 of the Artificial Intelligence Risk Classification Framework under Article 16 of the Artificial Intelligence Basic Act. It is addressed to the competent authorities for each industry, which follow its process when setting risk-based management rules under Article 16(2). It applies to civil-domain AI applications and excludes military use. The framework prescribes four steps. Authorities: • Take stock of AI applications in the sectors they oversee; • Identify risks against the risk type table; • Assess severity against the serious-harm examples to determine whether an application is high risk; and • Respond by planning promotion or management measures, reviewing their rules periodically. Risk is assessed on inherent characteristics, and the possibility of harm is sufficient. The mitigating effect of existing laws, administrative measures or technical means is disregarded until the response stage. Key elements include: • Twenty risk sub-types in three categories: technical design defects of the AI system itself (A1–A8), post-deployment operation and human-machine interaction problems (B1–B6), and social structure and environmental impact (C1–C6); • Sub-type B6 covers AI agents acting beyond their authorisation, including autonomously acquiring system access beyond the authorised scope, and chain reactions between agents in multi-agent systems; • An application is high risk under Article 17(1) where it may cause serious harm to national security, fundamental rights, life safety, property, social order or the ecological environment; • Management measures range from transparency labelling and mandatory disclosure of generative AI or deepfake content, through prior approval and third-party audit, to restriction or prohibition under Article 5(1) where risk cannot be effectively managed; • High-risk applications require clear warnings under Article 5(2) and clear attribution of liability, with remedy, compensation or insurance mechanisms under Article 17(1); and • Financial examples in the serious-harm annex include unlawful alteration of core financial databases, credit rating refusal without appeal or explanation, exclusion of specific groups from basic financial services, AI agents autonomously executing unauthorised financial transactions, and paralysis of national financial settlement and clearing systems. MODA will periodically review the risk type table against domestic and international research and international standards. MODA Issues AI Risk Classification Framework Setting Twenty Risk Sub-Types and a Four-Step Process for Competent Authorities | MODA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (3/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	FSC	**FSC Calls on Financial Institutions to Prepare for Cyberattacks Enabled by Frontier AI Models**	On 14 July 2026, FSC reminded financial institutions to prepare early for cyberattack risks from frontier AI models. It attached a paper, "Challenges and Strategic Recommendations for the Financial Industry in Responding to AI Attacks". The FSC named Claude Mythos Preview, which Anthropic disclosed in April 2026, as the trigger. It stated that such models can help identify vulnerabilities, work out how to exploit them and produce working attack code at scale. As a result, vulnerabilities can be found and turned into attacks faster, at greater scale and more reliably. The paper states that the time from disclosure of a flaw to its exploitation may shrink from days or weeks to hours. It adds that a "patch flood", in which many fixes are released at once, could overwhelm testing and deployment resources. The FSC stated that institutions should prioritise speeding up the measures in its Financial Cybersecurity Resilience Development Blueprint, issued at the end of 2025, with senior management leading the work. The paper sets out seven measures. The first five accelerate existing Blueprint directions, the sixth targets near-term readiness, and the seventh concerns medium- to long-term capability: • **Zero trust:** phishing-resistant multi-factor authentication, network segmentation and continuous verification, so that a single compromise does not spread across systems; • **Continuous monitoring:** moving from simply seeing alerts to detecting anomalies early, triaging quickly and containing incidents faster; • **Shift-left security:** building security requirements into development, testing and deployment, with stronger controls over software release pipelines; • **Third-party governance:** routine use of software bills of materials (SBOMs) to track software components, with patching service levels, reporting deadlines and fallback arrangements gradually agreed with critical suppliers; • **Joint defence:** tiered reporting thresholds and notification deadlines for high-risk vulnerabilities and major supply chain incidents, building on information sharing through the Financial Information Sharing and Analysis Center (F-ISAC); • **Short-term preparedness:** identifying priority services and internet-facing systems, assessing patching capacity, applying compensating controls such as isolation where systems cannot be patched immediately, and rehearsing shutdown and degraded-operation scenarios; and • **Defensive AI:** planning the use of AI for vulnerability detection, monitoring and incident response, while keeping human review, audit trails and the ability to switch off or roll back. The measures are framed as recommendations and carry no deadlines. The FSC stated it will continue to monitor frontier AI capabilities, international regulatory practice and industry needs. Where necessary, it will adjust its supervisory focus, reference guidance or public-private cooperation arrangements. FSC Reminds the Financial Industry to Strengthen Preparedness Against Frontier AI Model Attack Risks | FSC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (1/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	SEC	**SEC Consults on Draft Rules for Supervising Stablecoin Transactions and Enhancing Digital Asset Market Oversight**	On 7 August 2026, SEC and BOT met digital asset business operators (DA operators) to discuss supervising stablecoin transactions such as USDT and USDC (SEC News Release No. 165/2026). The authorities aim to reduce the risk of such transactions being used for money laundering, cybercrime or circumventing international money transfer rules, and the SEC expects regulations to be issued by end-2026. On 3 September 2026, the SEC Board approved supervisory principles at Meeting No. 11/2569 (News Release No. 183/2026). The SEC published Public Hearing Document No. Or Nor Dor. 57/2569 on 10 September and announced the consultation the next day (News Release No. 191/2026). Citing a continuous rise since 2023 in USDT trading and transfers through DA operators, with patterns that may serve as a channel for the same misuse, the SEC set a 15-day consultation period on grounds of urgency. Key proposals include: • Stablecoin transfers into or out of a customer's Thai DA operator account would be permitted only from or to an account or private wallet verified as the customer's own, not another person's; • Inbound and outbound transfers between that account and the customer's own foreign DA operator account or private wallet would each be capped at THB 5 million per day per person per DA operator and would have to match the customer's source of income and financial position, failing which enhanced customer due diligence would apply; • The cap would not apply to transfers between a customer's own accounts at SEC-supervised DA operators that both apply the Travel Rule, DA operators' own-name business transfers, BOT-supervised operators approved by the BOT case by case to use stablecoins, or market makers (MMs) for stablecoin/Thai baht pairs; • Digital asset brokers (DA Brokers) and dealers arranging off-platform transactions would face a THB 3 million minimum transaction value and have to disclose prices on their website or platform, and DA Brokers could not arrange off-platform transactions directly between customers; • Digital asset exchanges would have to disclose on their websites their MMs and the digital assets covered, and screen, monitor and review MMs' sources of digital assets and transaction purposes; • DA Brokers could not use liquidity providers (LPs) for stablecoin/Thai baht pairs, and LPs would have to meet anti-money laundering criteria, be supervised by a regulator in their country of establishment and be disclosed to customers with any conflicts of interest; • DA Brokers' source exchanges would have to be overseen by a regulator in their country of establishment, not merely able to operate lawfully there, with screening and monitoring comparable to LPs; and • The SEC could order DA operators breaching requirements to collect and disclose information to the SEC to rectify within a set period, and then to take or refrain from taking any action. SEC and BOT hold discussions with digital asset business operators to enhance supervision of stablecoin transactions and combat cybercrime | SEC SEC Board approves principles for enhancing the supervision of stablecoin transactions conducted through digital asset business operators | SEC SEC seeks public comments on proposed principles for supervising stablecoin transactions to mitigate financial fraud risks | SEC	Public consultation ended on 25 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (2/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	SEC	**SEC Consults on Draft Rules for Thai Crypto ETFs and Stricter Qualifications for Foreign Digital Asset Custodians of Funds**	On 21 August 2026, SEC published Public Hearing Document No. Or Nor Jor. 50/2569, on 11 draft notifications to establish and supervise crypto exchange-traded funds (crypto ETFs) in Thailand, and No. Or Nor Jor. 51/2569, on principles for revising the qualifications of foreign digital asset custodians (DA custodians) used by mutual funds (MFs) and private funds (PFs) investing in digital assets (News Release No. 171/2026, 24 August 2026). The drafts follow the principles consultation under Document No. Or Nor Jor. 16/2569 (10 April to 11 May 2026), in which most respondents agreed with the framework, while several, including asset management companies (AMCs) and mutual fund supervisors, raised practical constraints of relying mainly on onshore custody. On 16 June and 2 July 2026 respectively, the Capital Market Supervisory Board and the SEC Board approved a revised custody approach: crypto ETFs would primarily use DA custodians licensed in Thailand, with the SEC able to announce that foreign DA custodians may be used where necessary and appropriate. MFs and PFs investing in digital assets may currently use a foreign DA custodian with the same qualifications as one serving SEC-regulated digital asset business operators; the SEC proposes to add a supervisory-authority test aligned with the crypto ETF rules. Key proposals include: • A crypto ETF would be a passive ETF established and managed by an AMC, classified as an alternative investment fund and named after the single crypto asset it invests in, with average net exposure of at least 80% of net asset value each accounting year and no crypto exposure through derivatives; • Eligible crypto assets, initially Bitcoin and Ethereum, would be prescribed by the SEC, and a crypto ETF could not use its crypto assets to generate yield, directly or indirectly (including via a custodian that lends them out), unless permitted by notification; • A mutual fund supervisor holding a crypto ETF's crypto assets itself would need a Thai DA custodian licence, and any appointed custody agent would primarily be a Thai-licensed DA custodian; • Crypto ETFs would be listed and traded only on the Stock Exchange of Thailand, with non-institutional investors first requiring investor education and a two-way risk acknowledgement, and securities companies barred from granting margin loans for them; • MFs and PFs could invest in Thai and foreign crypto ETFs within existing investment limits; initially, the SEC would not permit products linked to foreign crypto ETFs, such as depositary receipts, and securities companies could facilitate foreign crypto ETF investment only for institutional and ultra-high-net-worth investors; • AMCs could delegate an MF's digital asset investment management only to a Thai-licensed digital asset fund manager; • DA custodians and other digital asset business operators with adequate financial standing, personnel and systems could register as mutual fund supervisors, for crypto ETFs only, under Section 121 of the Securities and Exchange Act B.E. 2535 (1992); and • A foreign DA custodian would have to meet the existing qualifications and be supervised by a Signatory A to the International Organization of Securities Commissions Multilateral Memorandum of Understanding or the regulator where it is established, if on an SEC list that may initially cover 11 jurisdictions: South Korea, Hong Kong SAR, Japan, France, Malaysia, Germany, Luxembourg, Liechtenstein, Singapore, the United States and Ireland. Draft notifications on the establishment and supervision of crypto ETFs in Thailand | SEC Principles for revising the qualifications of foreign custodians of mutual funds and private funds investing in digital assets | SEC Draft Regulations on the Establishment and Supervision of Crypto ETFs in Thailand | SEC	Public consultation ended on 20 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (3/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	SEC	**SEC Consults on Conditions for Intermediaries Taking Clients to Invest in Overseas Digital Asset Derivatives**	On 31 August 2026, SEC published Public Hearing Document No. Or Nor Por. 52/2569, proposing conditions for licensed derivatives agents and dealers that help clients invest in overseas derivatives based on digital assets. The proposal follows the SEC Board's decision in March 2026 to add digital assets, both cryptocurrencies and digital tokens, as underlying products under the Derivatives Act B.E. 2546 (2003). That decision allows intermediaries to offer digital asset derivatives in Thailand and to take clients to such products overseas. The SEC is also agreeing contract specifications for Thai digital asset derivatives with Thailand Futures Exchange (TFEX). The SEC stated that overseas digital asset derivatives vary widely in form and risk. Perpetual futures and contracts for difference mostly trade on unregulated overseas exchanges that have no central counterparty (CCP) to guarantee settlement. At present, intermediaries may offer retail and high-net-worth investors only overseas derivatives that resemble products tradable in Thailand. Ultra-high-net-worth and institutional investors face no such limits. Under the proposal, intermediaries could offer overseas digital asset derivatives to retail, high-net-worth and ultra-high-net-worth investors only where the product: • matches a digital asset derivative traded on TFEX in its underlying asset, contract term, leverage, and delivery or settlement method, with dated contracts required to run for at least one month; • is supervised by a regulator that is a Signatory A to the International Organization of Securities Commissions (IOSCO) Multilateral Memorandum of Understanding (MMoU), or that comes from an OECD or ASEAN Economic Community country, as under the current rules; • is offered in that regulator's home market, as under the current rules; and • trades on an exchange that clears through a CCP and is either supervised by an IOSCO MMoU Signatory A regulator or a member of the World Federation of Exchanges. Overseas digital asset derivatives that fall outside these conditions, including over-the-counter products, could be offered only to institutional investors. The SEC stated that institutional investors have the expertise to assess and manage complex, high-risk products. It added that the conditions are intended to give other investors protection in line with the products' risk. SEC Seeks Public Comments on Proposed Amendments to Regulations on Intermediaries' Facilitation of Clients' Investment in Digital Asset Derivatives Overseas | SEC	Public consultation ended on 30 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (4/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	SEC	**SEC Issues Travel Rule Requiring Digital Asset Business Operators to Transmit Originator and Beneficiary Information with Digital Asset Transfers**	On 2 September 2026, SEC announced in News Release No. 179/2026 that it has issued the "Travel Rule for Digital Assets" under Notification of the Office of the Securities and Exchange Commission No. Sor Thor. 9/2026 Re: Establishment of Risk Management Measures for the Transfer and Receipt of Digital Assets to Prevent the Use of Digital Asset Business Services as Channels for Money Laundering and Technology-Related Crimes, dated 25 August 2026. The notification follows a resolution of the Subcommittee on Financial Data Connectivity for Enhancing the Monitoring of Suspicious Financial Transactions that the SEC, together with the Anti-Money Laundering Office (AMLO), issue interim regulations for digital asset business operators (DA operators) while AMLO prepares regulations under the Anti-Money Laundering Act. The SEC consulted on the proposed principles during March–April 2026 and on the draft notification during June–July 2026, and reported that most stakeholders agreed with both. DA operators must establish policies and operating procedures for managing risks related to the transfer and receipt of digital assets, and collect information on customers and their counterparties in connection with digital asset transfers. They must also conduct due diligence on counterparties, verify the qualifications of the counterparty's digital asset service provider and of any intermediary DA operator in the transfer route, and verify ownership of, or control over, self-hosted wallets when transferring digital assets to or receiving them from such wallets. Ordering DA operators must transmit originator and beneficiary information together with the transfer order to the beneficiary's service provider. Information accompanying every digital asset transaction must be retained for at least five years in a manner that enables the supervisory authority to retrieve or examine it promptly. The regulations take effect on 27 February 2027, which the SEC stated allows DA operators time to prepare and develop systems for information transmission, receipt and transaction monitoring. SEC issues Travel Rule for Digital Assets to strengthen anti-money laundering and prevent technology-related crimes in line with international standards | SEC	Effective on 27 February 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (5/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	SEC	**SEC Consults on Draft Notifications Revising Net Capital Requirements for Digital Asset Business Operators to Support Domestic Trading and Custody**	On 11 September 2026, SEC published Public Hearing Document No. Or Nor Dor. 59/2569 (News Release No. 190/2026), seeking comments on 19 draft notifications, annexes and reporting forms. The drafts would revise the net capital (NC) requirements for digital asset business operators to support domestic trading and custody of customers' assets (local activities), together with related NC rules for securities and derivatives business operators. The SEC Board approved the principles at Meeting No. 6/2569 on 7 May 2026, and most respondents agreed with them in the consultation under Public Hearing Document No. Or Nor Dor. 27/2569 from 26 May to 25 June 2026. The revisions aim to promote local activities, reduce reliance on foreign service providers and ensure that capital reflects business risks. The draft notifications are expected to take effect on publication in the Royal Gazette. Key proposals include: • Operators maintaining capital under the NC-1 approach, namely digital asset exchanges (DA Exchanges), brokers (DA Brokers) and dealers, and digital asset fund managers and advisors holding customers' assets, would have counterparty, settlement and fund management risk added to the existing custody and trading service risk; • The counterparty risk charge on customers' assets prefunded or outstanding with another digital asset operator would be 8% of their value for a foreign and 1.5% for a domestic counterparty, with such holdings capped at 10% of total customers' assets, while rates for assets with digital asset custodians (DA Custodians) would remain 2% for foreign and 0.5% for domestic custodians; • The settlement risk charge would be 12% of the value of customers' assets pending settlement multiplied by the counterparty risk charge rate, unless a protective mechanism such as a third-party escrow custodian is in place, and the fund management risk charge 0.01% of net asset value, reducible by insurance cover; • DA Brokers could use SEC-supervised domestic DA Exchanges for order execution and custody of the resulting customers' digital assets, without their own custody system or hot and cold wallet proportions for that portion, subject to a 1.5% counterparty risk charge and conditions on exchange selection, written contracts, disclosure and reporting; • Participating DA Exchanges would have to use advanced wallet and key management technology, manage concentration in any single wallet, accept full liability for customers' digital assets lost or damaged through neglect of duty, and report customers' asset data to DA Brokers daily; • DA Custodians' cold wallet custody risk charge would be tiered at 0.5% on the first THB 100,000 million of customers' assets and 1% above that, with a segregated wallet for each customer; • Insurance offsetting NC for custody risk would cover only losses from hot and cold wallet custody, and qualifying digital tokens would be excluded from custody and counterparty risk calculations; and • For companies conducting securities or derivatives business alongside digital asset business, the SEC could order suspension of all digital asset business if the company fails to submit a capital remediation plan or resolve its capital shortfall, or its capital stays below 60% of the minimum calculated from the digital asset business alone for five consecutive days; the definitions of business operators would also widen to cover derivatives dealers and derivatives fund managers not conducting other business, and digital asset fund managers. Draft notifications revising the net capital (NC) rules for digital asset business operators to support domestic trading and custody of client assets, and related NC rules for securities and derivatives business operators | SEC SEC seeks public comments on draft notifications revising the NC requirements for digital asset business operators to support local activities | SEC	Public consultation ended on 11 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (6/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
6	**BOT**	**BOT Consults on Draft Security Guideline for Facial Recognition Used to Verify or Authenticate Financial Service Users**	On 14 September 2026, BOT opened a public consultation on a draft BOT Guideline on the Security of Biometric Technology of the Facial Recognition Type for Verifying or Authenticating Service Users. BOT stated that threats targeting facial recognition are becoming more sophisticated, particularly presentation attacks using AI deepfakes, which raise the risk of impersonation for unauthorised transactions. The draft would repeal the Guideline on the Use of Biometric Technology in Financial Services issued under BOT Circular No. Thor Por Thor. For Nor Chor. (09) Wor. 689/2566 dated 29 September 2023. It would apply to BOT-supervised providers that use facial recognition through mobile applications: financial institutions, specialised financial institutions, regulated payment service providers, and regulated personal loan and nano finance operators. Providers would be required to secure facial recognition systems, presentation attack detection (PAD) systems and biometric data across face data capture, signal processing, storage, face comparison and decision. Key proposals include: • Vulnerability assessments at least every three months and penetration tests at least annually, and on any significant change, with penetration tests covering at least presentation attacks, video injection attacks and attacks through APIs; • Event logs retained for at least 90 days, or as required by law, and protected against unauthorised alteration or destruction; • Verification refused on detection of a rooted or jailbroken device, an emulated environment, application tampering, a face image below the provider's quality criteria or a presentation attack; • Face data, biometric references and other personal data stored separately with at least logical separation, biometric data encrypted at rest and in transit and accessed with multi-factor authentication, and third-party providers not permitted to retain users' face data unless required by law; • A False Match Rate (FMR) of no more than 0.01% and an Impostor Attack Presentation Accept Rate (IAPAR) of no more than 4% for each type of attack instrument; • Performance tests under the annexed frameworks at least annually and on any significant change, using at least 300,000 test transactions and 776 test subjects for a target FMR of 0.01%, and PAD tests that include deepfake and live-stream video shown on a monitor of at least 3,840 × 2,160 pixels; and • Prior consultation with BOT before using other biometric types, such as iris or fingerprint recognition, or facial recognition for other purposes. Providers already using the technology would be required to complete the performance tests and a compliance assessment by internal audit or an independent external auditor, and report the results to BOT within 90 days from the day after the guideline is issued. Results obtained under the existing guideline could be reported if they are no more than one year old and consistent with the new requirements. Annual tests in later years would not need to be reported unless BOT requires it, and reporting under the existing biometric report form would cease from the day after issuance. Public consultation: (draft) guideline on the security of biometric technology of the facial recognition type for verifying or authenticating service users | BOT	Public consultation ended on 13 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (1/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**Government**	**Government Issues Administrative Penalties for Violations in the Pilot Crypto-Asset Market**	On 16 July 2026, the State Council issued Decree No. 284/2026/ND-CP on administrative penalties for violations relating to crypto assets and the crypto-asset market under the pilot established by Resolution No. 05/2025/NQ-CP of 9 September 2025 (Resolution 05). The Decree applies to Vietnamese and foreign organisations and individuals, including crypto-asset issuers, service providers and pilot investors. It covers offering and issuance, market organisation, service-provider duties, trading, foreign investor remittances, unlawful handling of account data, obstruction of inspections, and anti-money laundering (AML), counter-terrorist financing (CFT) and counter-proliferation financing (CPF) duties. Sanctions are a warning or a fine, capped at VND 200 million for organisations and VND 100 million for individuals; the tiers are set for organisations, and individuals pay half. Additional sanctions are deprivation of the right to use the market-organising service licence for 1 to 3 months, suspension of offering and issuance for 1 to 12 months, of service provision for 1 to 6 months and of trading for 1 to 12 months, and confiscation. Remedial measures include correcting information, disgorging unlawful gains, removing websites and trading systems, and cancelling offerings with full refunds. Highlights of the fine tiers for organisations include: • **Offering and issuance:** VND 70–100 million for breaching foreign ownership rules on underlying assets; VND 100–150 million for inaccurate, incomplete or untimely information; VND 150–200 million for offering to ineligible persons, offering without meeting Resolution 05 conditions, or failing to publish or follow the prospectus; • **Market organisation:** VND 70–100 million for failing to announce the official service start date within 7 working days of licensing; VND 150–180 million for failing to file licence adjustments or operating outside the licence; VND 180–200 million for providing services or advertising without a market-organising licence; • **Service providers:** VND 30–50 million for failing to publish required procedures, audited financial statements or fee schedules; VND 50–70 million for failing to verify investor identity; VND 100–150 million for failing to segregate client funds and assets or to monitor trading; VND 150–200 million for failures on prospectus accuracy, information technology security and client-asset protection; and VND 50–70 million (under 15 days late) or VND 70–100 million (15 days or more late) for late information disclosure; • **Trading:** VND 30–50 million for domestic investors trading outside licensed service providers; VND 70–100 million for domestic investors trading assets offered to foreign investors; • **Foreign investor remittances:** VND 30–50 million for foreign investors breaching account opening, closing and use rules; VND 70–100 million for inauthentic dossiers or untruthful declarations; for authorised banks, VND 50–70 million for reporting dedicated-account activity under 15 days late, and VND 70–100 million for reporting 15 days or more late, failing to check and keep transaction documents, or failing to issue internal rules; • **Account data and inspections:** VND 150–200 million for unlawfully collecting, trading or disclosing crypto-asset account data; VND 50–150 million for obstructing inspections; and • **AML/CFT/CPF:** VND 80–200 million, including VND 100–120 million for customer due diligence and risk-assessment failures, VND 150–200 million for failing to report suspicious or required large-value transactions or to issue internal rules, and VND 170–200 million for failing to delay transactions or freeze accounts and assets where required. Penalising authority sits with office-holders of the State Securities Commission, SBV, the Ministry of Public Security and provincial People's Committees, with fining powers of up to VND 100 million, VND 160 million or VND 200 million for organisations depending on the office; SBV office-holders may penalise only violations relating to foreign investor remittances, account data, obstruction of inspections and AML/CFT/CPF duties. Decree No. 284/2026/NĐ-CP on administrative penalties for violations related to crypto assets and the crypto asset market | Government	Effective on 1 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (2/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**National Assembly**	**National Assembly Passes Law No. 23/2026/QH16 Bringing Crypto-Asset Service Providers into Vietnam's Anti-Money Laundering Regime**	On 24 August 2026, Vietnam's National Assembly passed Law No. 23/2026/QH16 at the first extraordinary session of the 16th National Assembly. The law amends three statutes at once, including the Law on Anti-Money Laundering No. 14/2022/QH15, the Law on the State Bank of Vietnam No. 46/2010/QH12, and the Law on Credit Institutions No. 32/2024/QH15. The new rule adds crypto-asset service providers to the list of entities that must report under the anti-money laundering (AML) law. Those entities therefore take on the same customer due diligence, reporting and record-keeping duties as banks and other reporting entities. Key changes to the AML law include: • Crypto-asset services added as a reporting sector, with 15 crypto-specific indicators of suspicious activity, such as splitting transactions to stay under thresholds, using mixing or anonymity-enhancing services, and transfers to high-risk jurisdictions identified by the Financial Action Task Force (FATF); • A wider definition of beneficial owner that covers legal arrangements, plus new customer information requirements for trusts and similar arrangements; • A duty on trustees to collect and keep information on settlors, beneficiaries and controlling persons for at least five years after they cease acting; • Customer due diligence triggered by suspicion of money laundering even where a transaction is not completed, with no need to ask customers for information already held in national databases; • Life insurance beneficiaries to be identified when they are named and verified at the time of payout; • a money laundering risk assessment required before new products or services are launched, or before existing ones adopt new technology; • Protection from liability for anyone who reports in good faith, and whistleblower protections for people who supply AML information; and • Clearer supervisory roles, with the Ministry of Finance responsible for AML in the crypto-asset sector and inspecting crypto-asset reporting entities when the Government assigns it to. The amendments to the Law on the State Bank of Vietnam establish that transactions, payments, price listings, advertising, quotations and contract pricing in Vietnam may not be made in foreign currency unless a law, a National Assembly resolution or the State Bank's Governor permits it. They also allow the State Bank to apply different prudential ratios to individual institutions according to their risk, with those institutions required to follow a roadmap back to the standard ratios. Law No. 23/2026/QH16 of the National Assembly: Law on Amending and Supplementing a Number of Articles of the Law on the State Bank of Vietnam, the Law on Anti-Money Laundering, and the Law on Credit Institutions | National Assembly	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

ASIA PACIFIC CENTRE FOR REGULATORY STRATEGY (ACRS)

ACRS Co-leads



Nai Seng Wong
Partner, SEA
ACRS Chair
SEA Regulatory Strategy Lead



Shinya Kobayashi
Partner, Japan
JP Insurance Sector Leader



Sean Moore
Partner, Australia
AU SR&T FS Industry Lead



Lakshmi Narasimhan
Partner, India
India SR&T



Xu Du
Director, China
China SR&T

ACRS Core-team



Nicola Sergeant
Managing Director
Operations Lead
JP SR&T



Edwin Goh
Manager
Coordinator
SEA SR&T



Nusaybah Maszlee
Consultant
SEA SR&T

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Acknowledgements

Australia

Tony Zhi-Wei Tang
Associate Director
Deloitte Australia



Eric Kanikevich
Senior Consultant
Deloitte Australia



China Mainland

Cheryl Fan Jia
Manager
Deloitte China



Hong Kong SAR

Adelide Yeung
Partner
Deloitte China



Gianfran Liu
Partner
Deloitte China



Indonesia

Robertus Indrakrishna
Partner
Deloitte Indonesia



David Christian Hidayat
Director
Deloitte Indonesia



India

Satya Mahapatra
Partner
Deloitte India



Japan

Shoya Kusuda
Senior Consultant
Deloitte Japan



Malaysia

Prakash Arikrishnan
Partner
Deloitte Malaysia



Wai Theng Ha
Senior Manager
Deloitte Malaysia



Philippines

Herbert Rollom
Director
Deloitte Philippines



Anna Avila
Manager
Deloitte Philippines



New Zealand

Catherine Law
Partner
Deloitte New Zealand



Singapore

Samuel Yue Xuan Ang
Consultant
Deloitte Singapore



Taiwan (China)

Kelly Liu
Partner
Deloitte Taiwan



Chien Wang
Manager
Deloitte Taiwan



Thailand

Narumol Jirapanich
Partner
Deloitte Thailand



Boonsom Jarusiritarangkul
Partner
Deloitte Thailand



Vietnam

Tho Nguyen
Partner
Deloitte Vietnam



Quoc Anh Luu
Senior Manager
Deloitte Vietnam



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Appendix

Other Q3 2026 Frontier Technology Regulatory Updates

Australia (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**AUSTRAC**	**AUSTRAC Makes VASP Register Publicly Available to Verify Registered Virtual Asset Service Providers**	On 30 June 2026, the Australian Transaction Reports and Analysis Centre (AUSTRAC) made its register of virtual asset service providers (VASPs) publicly available, so that consumers, businesses and reporting entities can check whether a provider is registered before using its services. AUSTRAC Makes VASP Register Publicly Available to Verify Registered Virtual Asset Service Providers | AUSTRAC	-
2	**Treasury**	**Australian Treasury Releases Final Report of the Independent Review of the Enhanced Regulatory Sandbox**	On 1 July 2026, the Australian Treasury released the final report of the independent review of the Enhanced Regulatory Sandbox (ERS), which makes six recommendations in response to persistently low uptake, including repealing the ERS legislation and having the Australian Securities and Investments Commission (ASIC) use its existing relief powers more flexibly. Australian Treasury Releases Final Report of the Independent Review of the Enhanced Regulatory Sandbox | Australian Treasury Final Report on the Independent Review of the Enhanced Regulatory Sandbox | Australian Treasury	Government response expected in the second half of 2026.
3	**ASIC**	**ASIC Publishes Corporate Plan 2026–27 Naming AI Adoption, AI Market Integrity Risks and Frontier AI Among Its Priorities**	On 26 August 2026, ASIC published its Corporate Plan 2026–27, which names AI-driven market manipulation, deepfakes and the use of AI in customer-facing banking services among its areas of increased focus. ASIC Publishes Corporate Plan 2026-2027 to Name AI Adoption, AI Market Integrity Risks, and Frontier AI Among Its Priorities | ASIC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**PBOC, NDRC, MOST, MIIT, GACC, SAMR, NFRA, CNIPA, and NDA**	**Nine Departments Issue a Sci-Tech Finance Data Catalogue Covering 26 Indicators Across Eight Categories**	On 29 July 2026, the People's Bank of China (PBOC) and eight other departments issued a notice publishing a national catalogue of 26 sci-tech finance data indicators across eight categories, and launched a pilot of trusted data spaces for sci-tech finance. Nine Departments Issue a Sci-Tech Finance Data Catalogue Covering 26 Indicators Across Eight Categories | PBOC, NDRC, MOST, MIIT, GACC, SAMR, NFRA, CNIPA and NDA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	HKMA FSTB	**FSTB and HKMA Conclude Phase One of DLT Fixed Income Review and Confirm Companies Ordinance Accommodates Tokenised Bond Registers**	On 29 June 2026, HKMA and the Financial Services and the Treasury Bureau (FSTB) concluded phase one of their joint review of distributed ledger technology (DLT) in Hong Kong's fixed income market, finding the existing legal and regulatory environment sufficiently flexible for tokenised bond issuance, while CR confirmed in Frequently Asked Questions that a debenture holders' register maintained on DLT satisfies the record-keeping requirements of the Companies Ordinance (Cap. 622). FSTB and HKMA Conclude Phase One of DLT Fixed Income Review and Confirm Companies Ordinance Accommodates Tokenised Bond Registers | FSTB and HKMA	Phase two to commence in the second half of 2026.
2	HKMA	**HKMA Deputy Chief Executive Urges Post-Quantum Readiness and Workforce Reskilling at HKMA–HKAB Quantum Computing Seminar**	On 6 July 2026, HKMA Deputy Chief Executive Arthur Yuen stated at the HKMA–Hong Kong Association of Banks (HKAB) quantum seminar that banks must be ready for post-quantum cryptography (PQC) before the first attacks occur, and that the HKMA will monitor each bank's Quantum Preparedness Index (QPI). HKMA-HKAB Seminar on Quantum Computing—Opening Remarks by Deputy Chief Executive | HKMA	-
3	MPFA	**MPFA Introduces Step-Up Authentication and Facial Identification for eMPF Withdrawal Applications**	On 26 July 2026, the Mandatory Provident Fund Schemes Authority (MPFA) announced that eMPF withdrawal applications will require step-up authentication through iAM Smart with real-time facial identification, except for small-balance and death claims. MPFA Introduces Step-Up Authentication and Facial Identification for eMPF Withdrawal Applications | MPFA	Step-up authentication to be introduced at the end of July 2026.
4	HKMA	**HKMA Executive Director Opens FiNETech8 on Quantum Readiness**	On 27 July 2026, HKMA Executive Director Carmen Chu opened FiNETech8, announcing the quantum whitepaper and the QPI, and identifying cryptographic agility, meaning the ability to upgrade algorithms without major disruption, as the whitepaper's key recommendation. HKMA Executive Director Opens FiNETech8 on Quantum Readiness | HKMA	-
5	HKMA SC IA MPFA	**HKMA, SFC, IA and MPFA Announce First Cohort of GenA.I. Sandbox++ Focused on Agentic AI**	On 27 August 2026, Hong Kong's four financial regulators announced the first cohort of the GenA.I. Sandbox++, comprising 36 use cases from 30 financial institutions and 27 technology partners, focused on agentic AI and on AI overseeing other AI. First cohort of Gen A.I. Sandbox++ | HKMA First cohort of Gen A.I. Sandbox++ | SFC	Technical trials scheduled to begin later in 2026.
6	HKSAR	**Chief Executive's 2026 Policy Address Sets Out the Digital Asset and Artificial Intelligence Governance Agenda**	On 16 September 2026, Hong Kong's Chief Executive set out digital asset measures, including regulated stablecoin trading and tokenisation tests for Exchange Fund Bills, together with a new Commissioner for AI to support the government's coordination of AI governance. Chief Executive's 2026 Policy Address Sets Out the Financial Services, Digital Asset and Artificial Intelligence Governance Agenda | HKSAR	Society-wide AI agent safety guidelines planned for 2027.

Indonesia (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**OJK**	**OJK Reports Preparation of a 2026–2031 Roadmap for Financial Sector Technology Innovation, Digital Financial Assets and Crypto Assets**	On 2 July 2026, OJK stated that it is preparing a 2026–2031 roadmap for financial sector technology innovation, digital financial assets and crypto assets, built on the principles of affordability, integrity, agility and sovereignty. OJK Reports Preparation of a 2026–2031 Roadmap for Financial Sector Technology Innovation, Digital Financial Assets and Crypto Assets | OJK	-
2	**OJK**	**OJK Promotes Two Accelerator Programmes for Financial Technology and Creative Economy Startups**	On 23 July 2026, OJK announced two 2026 startup accelerator programmes under its OJK Infinity innovation centre, focused on AI, fraud detection and real-world asset tokenisation on the fintech side, and on intellectual property tokenisation and Web3 on the creative economy side. OJK Promotes Two Accelerator Programmes for Financial Technology and Creative Economy Startups | OJK	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	MOJ	**MOJ Study Group Drafts Report Confirming Voice Falls Within Publicity Rights Protection Against Generative AI Misuse**	On 27 July 2026, a Ministry of Justice (MOJ) study group considered a draft report concluding that a person's voice is protected by publicity rights against unauthorised imitation by generative AI. MOJ Publishes Draft Report Confirming Voice Falls Within Publicity Rights Protection Against Generative AI Misuse | MOJ	-
2	JFSA	**JFSA Publishes Analytical Report on IT Resilience in the Financial Sector**	On 30 July 2026, the Financial Services Agency (JFSA) published its analytical report on IT resilience in the financial sector, covering system failures, AI-enabled cyber threats, third-party risk and lessons from cloud resilience exercises. Publication of Analytical Report on IT Resilience in the Financial Sector | FSA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

New Zealand (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**FMA**	**FMA Launches Thematic Review of Artificial Intelligence in Financial Advice**	On 6 August 2026, the Financial Markets Authority (FMA) launched an exploratory thematic review of how AI is used in financial advice, which it stated is intended to build shared understanding rather than to assess compliance. FMA Launches Thematic Review of Artificial Intelligence in Financial Advice | FMA	Survey responses closed on 18 September 2026.
2	**MBIE**	**MBIE Assumes Governance and Delivery of the Consumer Data Right Standards as Open Banking Volumes Rise**	On 21 August 2026, the Ministry of Business, Innovation and Employment (MBIE) confirmed it will take over the open banking standards under the Consumer Data Right from Payments NZ, as monthly regulated open banking payments passed 408,000 transactions worth NZD 130 million. MBIE Assumes Governance and Delivery of the Consumer Data Right Standards as Open Banking Volumes Rise | MBIE	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**SEC**	**SEC Launches VERITAS Giving Blockchain-Signed Corporate Documents the Force of Notarised Documents**	On 27 July 2026, the Securities and Exchange Commission (SEC) launched VERITAS, an optional blockchain platform whose signed documents carry the same legal effect as notarised documents, unless a law specifically requires notarisation. SEC Launches VERITAS Giving Blockchain-Signed Corporate Documents the Force of Notarised Documents | SEC	Effective on 28 July 2026.
2	**BSP**	**BSP Issues Guidelines Giving Eligible Rural Banks a Free Three-Year Cloud Core Banking System Subscription**	On 12 August 2026, the Bangko Sentral ng Pilipinas (BSP) set out guidelines offering eligible rural banks free technical assistance to move from legacy systems to a cloud-hosted core banking system, including a 36-month subscription. BSP Issues Guidelines Giving Eligible Rural Banks a Free Three-Year Cloud Core Banking System Subscription | BSP	Applications opened on 12 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (1/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	MAS	**MAS Partners Industry to Develop Safeguards for AI Agents Operating in Finance**	On 3 July 2026, MAS, together with financial institutions and FinTechs under the BuildFin.ai initiative, published the white paper "Safeguards for Agentic Finance at Runtime (SAFR)", proposing an industry-developed governance framework of checkpoints that verify and record AI agents' proposed actions before task execution. MAS Partners Industry to Develop Safeguards for AI Agents Operating in Finance | MAS Safeguards for Agentic Finance at Runtime (SAFR) | MAS	-
2	PDPC	**PDPC Issues Guidance on Applicability of PDPA to Ant International's Privacy-Preserving Payment Risk Control Proof-of-Concept**	On 7 July 2026, PDPC published practical guidance on the applicability of the Personal Data Protection Act (PDPA) to Ant International's proof of concept on privacy-preserving payment risk controls using multi-party computation, addressing whether the data exchanged in the workflow constitutes personal data. PDPC Issues Guidance on Applicability of PDPA to Ant International's Privacy-Preserving Payment Risk Control Proof-of-Concept | PDPC	-
3	IMDA	**IMDA Issues Voluntary Transparency Guidelines for Generative AI Chatbots, with Major Singapore Banks Among Early Adopters**	On 20 July 2026, IMDA published voluntary Transparency Guidelines for Generative AI Chatbots, centred on a "chatbot info card" and the principles of relevance, accessibility and timeliness, with Google, Meta, DBS, OCBC, Singapore Airlines and Synapxe indicating that they will use the Guidelines as a point of reference. IMDA Issues Voluntary Transparency Guidelines for Generative AI Chatbots, with Major Singapore Banks Among Early Adopters | IMDA	Early adopters indicate transparency improvements over the next 12 months.
4	PDPC	**PDPC Launches Guide on Federated Learning to Support Privacy-Preserving Collaborative AI Development**	On 20 July 2026, PDPC launched a guide on federated learning, a technique for training AI models across several organisations' data without pooling the underlying data, together with an adoption roadmap. PDPC Launches Guide on Federated Learning to Support Privacy-Preserving Collaborative AI Development | PDPC	-
5	MAS	**MAS Hosts 31st EMEAP Governors' Meeting Covering AI Risks to Regional Financial Systems**	On 23 July 2026, MAS hosted the 31st Executives' Meeting of East Asia-Pacific Central Banks (EMEAP) Governors' Meeting, where Governors discussed the financial stability risks of large AI investments and resolved to deepen exchanges on digital fraud and scams. 31st Executives' Meeting of East Asia-Pacific Central Banks (EMEAP) Governors' Meeting | MAS	-
6	MAS ABS	**MAS and ABS Establish Taskforce to Strengthen Cyber and Technology Resilience against AI-Driven Threats**	On 28 July 2026, MAS and the Association of Banks in Singapore (ABS) announced an industry taskforce, including DBS, OCBC, UOB and Singapore Exchange, to strengthen collective resilience against cyber threats from frontier AI models. MAS and ABS Establish Taskforce to Strengthen Cyber and Technology Resilience against AI-driven Threats | MAS and ABS	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (2/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	MAS	**MAS Board Member Highlights Actuaries' Role in AI Governance at the Asian Actuarial Conference**	On 19 August 2026, MAS Board member Alvin Tan stated that actuaries have a role in challenging assumptions, identifying biases and testing AI tools so that they are robust, explainable and properly governed. "Navigating New Tools, New Terrain and New Needs" - Opening Address by Mr Alvin Tan, Minister of State, Ministry of Foreign Affairs and Ministry of National Development, and Board member of MAS, at the Asian Actuarial Conference on 19 August 2026 | MAS	-
6	MAS	**MAS Insurance Department Executive Director Identifies AI Among Developments Reshaping the Insurance Sector**	On 20 August 2026, Daniel Wang, Executive Director of MAS' Insurance Department, stated that AI is changing how insurers assess risk, serve customers and manage claims. Keynote Address by Daniel Wang, Executive Director, Insurance Department, Monetary Authority of Singapore, at Singapore College of Insurance Graduation Ceremony 2026 on 20 August 2026 | MAS	-
7	MAS	**MAS Commits SGD 220 Million to Support Next Phase of FinTech Innovation**	On 31 August 2026, MAS committed SGD 220 million over three years under the renewed Financial Sector Technology and Innovation Scheme (FSTI 4.0), with six funding tracks focused on AI, distributed ledger technology and quantum technology. MAS Commits SGD 220 Million to Support Next Phase of FinTech Innovation | MAS	-
8	MAS	**MAS Managing Director Outlines AI, Cyber Resilience and Quantum Priorities at Global FinTech Fest 2026**	On 11 September 2026, MAS Managing Director Chia Der Jiun stated that AI is already widely used across Singapore's financial sector, that tokenisation may take a few more years to scale, and that it is not too early to prepare for quantum resilience. "Building the Financial System of the Future: Trusted, Connected and Resilient" – Special Address by MAS Managing Director at the Global FinTech Fest 2026 | MAS	Findings from the cross-institution AI-based scam and fraud detection work expected by end-2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	FSC	**FSC Amends Fraud Prevention Rules to Add Cross-Sector Inquiries and an Anti-Fraud Platform**	On 20 July 2026, FSC amended its fraud prevention rules for deposit-taking institutions, electronic payment institutions, credit card institutions and virtual asset service providers. The amendments let institutions query suspected fraud accounts across sectors and set up a cross-institution anti-fraud platform. They also allow any judicial police agency to instruct refunds to victims, including from the sale of virtual assets left in warned accounts. FSC Amends Fraud Prevention Rules to Add Cross-Sector Inquiries and an Anti-Fraud Platform | FSC Explanatory Statement and Comparison Table for the Amendment to the Fraud Prevention Regulations for Financial Institutions and Virtual Asset Service Providers | FSC	Effective on 20 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

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.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organisation"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organisation") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 415,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, or the Deloitte organisation is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

© 2026 Deloitte Touche Tohmatsu
Designed by CoRe Creative Services. RITM2672151