waystone | Compliance Solutions

Regulatory Update

APAC, April 2026

Issued 05 May 2026

Regulatory Updates – April 2026

Singapore

23 April 2026 – MAS Supervisory Priorities for Capital Markets Entities

The Monetary Authority of Singapore (MAS) has issued a circular (CMG 01/2026) setting out its supervisory priorities for Capital Markets Entities (CMEs) for 2026/27. The circular highlights three key focus areas: strengthening trust, culture and customer outcomes; operational, technology and cyber resilience; and financial resilience.

A consistent theme across MAS' priorities is the importance of strong governance, robust risk management, and the effective execution of controls supported by reliable data and robust technology systems. Applied in a risk-proportionate manner, these enable CMEs to address risks, grow sustainably and remain competitive in a rapidly evolving operating environment.

Strengthening Trust, Culture, and Customer Outcomes

In relation to AML/CFT, MAS acknowledges the industry's commitment to upholding robust standards while remaining mindful of the need for CMEs to provide efficient services and facilitate legitimate business access. MAS will continue working with the industry to provide clarity on risk-proportionate AML/CFT practices so that customers can transact more smoothly without weakening safeguards.

On culture and conduct, MAS intends to publish an information paper on essential culture capabilities that CMEs should build. Additional focus areas include:

- Consistent implementation of the Guidelines on Fair Dealing, with MAS sharing findings from its examinations of complaints management practices at key retail banks and insurers;
- Enhanced delivery of financial services to seniors and simplified estate administration procedures, in collaboration with The Central Depository (Pte) Limited and the Association of Banks in Singapore; and
- Continued anti-scam efforts, including new authentication solutions, an AI-enabled fraud detection pilot, reinforced PayNow protections and enhanced controls to prevent unauthorised trading in retail broking accounts.

Operational, Technology and Cyber Resilience

MAS continues to work with CMEs to improve operational resilience through four key pillars: operational risk management; technology and cyber risk management; third-party risk management; and business continuity management.

MAS recently consulted on updated Guidelines on Operational Risk Management and proposed Guidelines on Third-Party Risk Management. It will subsequently consult on updates to the MAS Notices on Technology Risk Management to cover IT asset management and continuous system monitoring.

On AI, MAS notes that rapid advances have increased the risk of software vulnerabilities being exploited. CMEs are encouraged to intensify cyber defence efforts through proactive vulnerability identification and timely security patching. MAS will also finalise the Guidelines on AI Risk Management this year, covering

fundamental frameworks, policies and procedures, as well as the capabilities CMEs need for responsible AI use.

Financial Resilience

Given economic uncertainty, CMEs should continue to manage business and financial risks proactively. For fund management companies (FMCs) specifically:

- MAS has consulted on updated Guidelines on Liquidity Risk Management for FMCs, which will strengthen alignment between redemption terms and fund asset liquidity and reinforce governance and disclosures on liquidity management tools; and
- MAS published the final Guidelines on Transition Planning for FMCs in March 2026, with FMCs expected to continue engaging investee companies on climate-related risks and to improve climate data collection and scenario analysis.

Looking Ahead

MAS remains committed to ensuring that its regulatory and supervisory approaches remain appropriately calibrated to a diverse range of business models and risks. It will continue to leverage technology to sharpen risk surveillance of CMEs and to support more targeted intervention efforts. MAS will also continue to partner the industry – for example, measures introduced under the Equities Market Review are moving Singapore decisively towards a more disclosure-based regime to support the sustainable growth of its equity market.

17 April 2026 – Advisory on Measures Against AI-Driven Threats (MAS/TCRS/2026/04)

The Monetary Authority of Singapore (MAS) has issued an advisory (MAS/TCRS/2026/04) on measures against AI-driven threats, in response to significant recent advances in frontier AI models that present new and heightened cyber security risks to financial institutions (FIs).

MAS highlights that recent developments – including the release of frontier AI models with autonomous capabilities to independently discover, chain and exploit security vulnerabilities – mark a pivotal shift where autonomous AI-driven attacks have progressed significantly over previous models. These advancements significantly compress the timeline from vulnerability discovery to exploitation. FIs should be prepared for the possibility that such capabilities, if widely available, could be misused by malicious actors to launch attacks that are faster, more adaptive and more automated than current campaigns.

Recommended Measures

MAS sets out key recommended measures for FIs:

- Validate basic cyber hygiene as a priority – FIs must validate that fundamental cyber hygiene controls are firmly in place, including securing identities (particularly privileged ones) with multi-factor authentication, applying security patches in a timely manner, ensuring malware protection is properly enabled, hardening systems using security standards, and maintaining effective network defences including appropriate network segmentation;
- Prioritise, optimise and accelerate vulnerability and patch management – FIs should review existing vulnerability and patch management policies to assess whether they can keep pace with compressed exploitation windows driven by AI-driven reconnaissance. Where patches cannot be applied immediately, compensating controls such as virtual patching should be considered. FIs should

maintain comprehensive inventories of external-facing assets and open-source libraries and third-party dependencies to enable rapid prioritisation and response;

- Maintain resilience for both systems and cyber resources – FIs should maintain immutable backups and regularly tested disaster recovery procedures. FIs should also plan for sustained cyber resourcing, including greater use of automation and risk-based prioritisation, to ensure sufficient capacity to remediate vulnerabilities, accelerate patch deployment, and strengthen detection and response capabilities;
- Leverage AI capabilities and automation for cybersecurity – FIs should evaluate harnessing AI capabilities in a responsible and controlled manner, adhering to security-by-design principles. AI integration should be considered across risk assessment (validating vulnerabilities and prioritising critical findings), threat modelling (enumerating attack paths and proposing kill chains), secure design and software development, security testing including source code reviews and adversarial simulations, and security detection and incident response; and
- Strengthen collaboration amongst cybersecurity groups – FIs should remain engaged in trusted information-sharing groups and enhance collaboration across the industry, enabling earlier detection and faster containment through the sharing of timely threat intelligence, including indicators of compromise, adversary tactics, AI-driven social engineering patterns and emerging exploitation trends. Collaboration should extend to third-party risk monitoring and management.

FIs are also expected to continuously monitor material developments and updates to AI models that may affect the threat landscape, including seeking timely access to relevant defensive offerings, monitoring advisories and threat bulletins released by industry associations and cybersecurity communities, and tracking related regulatory advisories to ensure that defensive measures remain current.

FIs are advised to read this advisory in conjunction with the MAS Notice on Cyber Hygiene, MAS Technology Risk Management Guidelines, other MAS related advisories, and the CSA Advisory on Risks associated with Frontier AI Models.

8 April 2026 – Advisory on Strengthening Cyber Security Posture (MAS/TCRS/2026/03)

The Monetary Authority of Singapore (MAS) has issued an advisory (MAS/TCRS/2026/03) on strengthening cyber security posture through effective risk governance, assurance and security practices. The advisory highlights useful practices for protecting against the latest cyber threats and addresses control gaps and weaknesses that have led to successful breaches over the past year.

MAS notes that in several recent breaches, affected organisations had deprioritised cyber security in favour of business performance and convenience, leaving their IT infrastructure vulnerable. It is therefore important that Boards and Senior Management set the right tone from the top to ensure effective IT governance and oversight, and instil strong IT risk culture and awareness.

Cyber Risk Governance

Financial institutions (FIs) are expected to put in place a robust IT governance structure and risk management framework, and ensure that key decisions involving trade-offs between business needs and cyber security are approved by Senior Management. MAS emphasises that FIs should go beyond a compliance-based mindset and adopt a risk-focused approach. Key governance expectations include:

- Ensuring that the Chief Information Security Officer ("CISO"), Head of IT Security, or equivalent is empowered and equipped with requisite resources and competency to effectively discharge their cyber security responsibilities; and
- Leveraging the Three Lines of Defence model to ensure clear risk ownership, effective risk management, and assurance on the state of cyber security controls, with adequate resourcing and skills across each line.

Cyber Security Practices

Threat actors, including advanced persistent threats, often target weaknesses in basic cyber hygiene to obtain an initial foothold before accessing critical systems. MAS identifies the following key areas where control weaknesses have led to successful attacks:

- IT Asset, Inventory and Configuration Management – FIs should maintain an up-to-date inventory of IT assets (including hardware, software, network and cryptographic components), implement regular network scanning and asset reconciliation processes, and maintain updated system and network documentation to facilitate effective monitoring, vulnerability management, patch management and incident response;
- Network Segmentation and Access Control – FIs should segregate production networks into subnets, implement network access controls, and deploy measures to detect anomalous traffic and block unauthorised connections, with administrative activities conducted on a separate out-of-band network;
- Privileged Identity and Access Management – FIs should restrict access to administrative and privileged accounts on a need-to-use basis, implement centralised privileged access management tools, role-based access control and multi-factor authentication, and conduct regular reviews of privileged activity logs;
- Threat Detection and Mitigation – FIs should deploy Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) solutions, or equivalents, to detect suspicious activities and support automated threat mitigation, investigation and remediation; and
- Centralised Security Monitoring – FIs should aggregate and correlate security events from different sources into centralised monitoring platforms to improve detection of security anomalies and timeliness of responses.

Cyber Security Assurance and Testing

FIs should conduct regular security testing to assess the effectiveness of cyber security controls and identify areas for improvement. Testing can include vulnerability assessments, penetration testing and adversarial attack simulations, as well as table-top exercises. MAS also encourages FIs to consider:

- Attack Surface Management (ASM) – a managed service that performs discovery and scanning of an organisation's publicly accessible digital assets, including cloud services and vendor/partner-connected tools, to proactively identify unpatched vulnerabilities and insecure configurations; and
- Bug Bounty Programmes (BBP) – structured programmes engaging external experts to discover and report vulnerabilities, complementing internal testing to achieve more extensive security coverage.

FIs are advised to read this advisory in conjunction with the MAS Notice on Cyber Hygiene and MAS Technology Risk Management Guidelines, and implement appropriate measures commensurate with the size, scale and criticality of their systems and operations. Where relevant, the measures should also be applied to third-party arrangements involving technology or digital services.

Hong Kong

09 April 2026 – Circular to Licensed Corporations which are Participants of The Stock Exchange of Hong Kong Limited or Hong Kong Futures Exchange Limited - Licence Holders Insurance Scheme for Exchange Participants

On 09 April 2026, the Securities and Futures Commission (SFC) issued a circular to licensed corporations which are participants of The Stock Exchange of Hong Kong Limited or Hong Kong Futures Exchange Limited setting out the arrangements of the Licence Holders Insurance Scheme for Exchange Participants for the scheme year from 1 April 2026 to 31 March 2027 (both dates inclusive) (circular).

The SFC circular applies to the following categories of licensed corporations:

- Category 1: Participants of The Stock Exchange of Hong Kong Limited and licensed for Type 1 regulated activity
- Category 2: Participants of Hong Kong Futures Exchange Limited and licensed for Type 2 regulated activity.

Under the Securities and Futures (Insurance) Rules, these corporations are required to take out and maintain insurance covering specified risks for the prescribed minimum amounts.

Key arrangements of the scheme:

- Marsh (Hong Kong) Limited has been re-appointed as insurance broker and scheme administrator.
- Two master policies provide an indemnity limit of $15 million per regulated activity per year, subject to a $3 million deductible per claim.
- Premium allocation methodology remains unchanged from the previous year, with premium loadings for claims and discounts available for large Category 2 participants based on turnover.

Marsh will issue debit notes and insurance documents separately. Licensed corporations must ensure they take out and maintain the required insurance under the Securities and Futures (Insurance) Rules.

For assistance or if you have any enquiries about this circular, please contact Waystone.

To view the circular, please click here.

20 April 2026 – Circular on secondary trading of tokenised SFC-authorised investment products

On 20 April 2026, the Securities and Futures Commission (SFC) issued a circular setting out the requirements under which the SFC would consider allowing secondary trading of tokenised SFC-authorised investment products (Tokenised Products) by the public in Hong Kong. (**circular**)

This circular should be read in conjunction with the Circular on tokenisation of SFC-authorised investment products and the Circular on intermediaries engaging in tokenised securities-related activities dated 20 April 2026 (revised) and 02 November 2023, respectively. It primarily facilitates on-platform secondary trading (on-screen auto-matching) of SFC-authorised open-ended funds on SFC-licensed virtual asset trading platforms (VATPs) to improve liquidity and tradability.

Key notes:

- Secondary trading of Tokenised Products may be offered to retail investors via on-platform trading (on-screen auto-matching) provided by SFC-licensed VATPs.
- Secondary trading must follow existing VATP Guidelines.
- Trades may be executed only when client's account has sufficient capital or product holdings of equivalent trading fungibility.
- SFC-licensed VATPs must implement fair pricing controls, including Price Deviation Alerts from indicative NAV, primary market alternatives, and pre/post-trade monitoring to prevent excessive fluctuations or manipulation.
- Product Providers should use their best endeavours to arrange at least one market maker (with a minimum 3-month notice for termination), monitor liquidity, maintain contingency plans, and appoint SFC-licensed distributors for creation/redemption.
- Enhanced disclosures are required on secondary trading risks (liquidity, price deviation, market maker reliance, price fragmentation), trading arrangements, fees, NAV information, and market making incentives.
- Product Providers and intermediaries (including VATPs and Connecting Brokers) must give early alerts and immediate notifications to the SFC and investors on any suspension or disruption of trading/market making.
- Prior consultation with the SFC (and approval for existing products) is required before launching or making material changes to secondary trading arrangements.

For assistance or if you have any enquiries about this circular, please contact Waystone.

To view the circular, please click here.

20 April 2026 – Circular on tokenisation of SFC-authorised investment products (Revised on 20 April 2026)

On 20 April 2026, the Securities and Futures Commission (SFC) issued a circular setting out the requirements for tokenisation of SFC-authorised investment products for public offering in Hong Kong. (circular).

The circular adopts a "see-through" approach and permits primary dealing (subscription/redemption) of tokenised SFC-authorised investment products, subject to additional safeguards. Secondary trading is covered in a separate circular issued on the same date.

Key notes:

- Product Providers remain ultimately responsible for the tokenisation arrangement, ownership records, cybersecurity and business continuity.
- Public-permissionless blockchains generally require additional controls.
- Offering documents must clearly disclose the tokenisation arrangement (including whether settlement is off-chain or on-chain), ownership representation and associated risks (cybersecurity, system outages, technical flaws, evolving regulations, etc.).
- Distributors must be SFC-licensed corporations or registered institutions.

- Product Providers must have at least one competent staff member with relevant tokenisation expertise to operate/supervise the tokenisation arrangement and manage related risks.
- Prior consultation with the SFC is required for new or existing tokenised products (approval may be needed for material changes).

For assistance or if you have any enquiries about this circular, please contact Waystone.

To view the circular, please click here.

Stay informed with our Regulatory Update

Navigate the ever-evolving regulatory landscape with our Regulatory Update. Our team of compliance experts provide a monthly review of a wide range of global regulatory compliance matters, including news, guidelines and significant regional updates. To sign-up to receive these updates, please follow the link below.

Find out more →

About Waystone

Waystone is a leading global provider of institutional governance, administration, risk, and compliance services to the asset management and financial services industry. Our global Compliance Solutions team helps clients navigate the regulatory landscape with confidence, aligning investment strategies and operational processes with compliance requirements. With over 100 compliance specialists based across Asia, the Middle East, Europe, and North America, we offer a comprehensive range of solutions, from company registration and licensing to compliance programmes and ongoing support.

In Singapore and Hong Kong, Waystone brings over 20 years of experience, working with clients regulated by the Monetary Authority of Singapore and the Securities and Futures Commission. Our team is well-equipped to provide bespoke, risk-focused, and cost-effective solutions. With extensive experience, we deliver the expertise you need while adding value to your corporate governance standards.

If you would like to discuss the themes raised in this guide with one of our APAC Compliance Solutions team members and learn how we can assist you, please contact us using the details below.

Contact us →