waystone | Compliance Solutions

Regulatory Update

APAC, July 2026

Issued 6 August 2026

Regulatory Updates – July 2026

Singapore

2 July 2026 – Guidelines – Liquidity Risk Management Practices (Fund Management Companies)

The Monetary Authority of Singapore (MAS) has revised its Guidelines on Liquidity Risk Management (LRM) Practices for Fund Management Companies (FMCs), with effect from 2 July 2026, following the consultation which concluded in February 2026. The revisions strengthen MAS' expectations on liquidity risk management and align Singapore's framework with recent international standards issued by IOSCO and the Financial Stability Board. The following are key changes:

1. **Anti-Dilution Tools (ADTs)** – Greater emphasis on ADTs including swing pricing, anti-dilution levies in addition to redemption gates or suspension of redemptions.

2. **Margin and collateral call liquidity risks** – Consider liquidity demands arising from margin calls, collateral calls and derivative exposures, in addition to investor redemptions.

3. **Product design requirements** – Assess liquidity risks at the fund design stage and ensure redemption terms, liquidity management tools and underlying asset liquidity are appropriately aligned.

4. **Liquidity cost allocation** – Detailed expectations apply to how liquidity costs (including bid-ask spreads and market impact costs) should be borne by transacting investors and how FMCs should estimate and calibrate such costs.

5. **Stress testing** – Stress testing should include multiple concurrent stress events, including market liquidity deterioration, counterparty failures, margin/collateral calls and redemption shocks, rather than focusing primarily on redemption scenarios.

6. **Governance and documentation standards** – There is greater emphasis on Board and senior management oversight, documented decision-making for liquidity management tools, contingency planning and escalation procedures.

7. **Investor disclosures** – FMCs should provide clearer disclosures on liquidity risks, redemption terms, lock-ups, settlement periods, liquidity management tools and the circumstances under which such tools may be activated.

FMCs should review their existing liquidity risk management frameworks, fund documentation, stress testing methodologies, investor disclosures and liquidity management tools to assess whether enhancements are required to align with the revised MAS expectations.

Please refer to the revised LRM Guidelines at this link.

16 July 2026 – Guidelines on Audit of Payment Service Providers

On 16 July 2026, the Monetary Authority of Singapore (MAS) issued the Guidelines on Audit of Payment Service Providers (PS-G04), setting out its supervisory expectations for the annual audits of licensed payment service providers (PSPs). While annual audits are already required under the Payment Services Act (PSA), the new guidelines provide greater clarity on MAS' expectations regarding audit scope, reporting and governance. The guidelines will apply to annual audits for financial years ending 31 December 2026 onwards.

The key expectations are as follows:

1. **Annual PSP audit requirements** – All licensed PSPs must appoint an external auditor annually and submit audited financial statements, an Independent Assurance Report and audit findings to MAS within 6 months of financial year-end.

2. **Single Auditor responsibility** – The same external auditor should perform the financial audit, Independent Assurance Report and regulatory audit findings, rather than using different auditors for different components.

3. **Management letters** – Audit findings, observations, recommendations, audit coverage and sample testing results must be submitted to MAS as part of the annual submission.

4. **Immediate notification of serious breaches** – PSPs and auditors are expected to immediately report significant breaches or control failures (e.g. safeguarding failures, base capital breaches, unlicensed activities and severe control weaknesses).

5. **Annual audit coverage** – Audits must cover safeguarding of customer monies/assets, PSN04 reporting accuracy, base capital compliance, compliance with exemption criteria (where applicable) and remediation of prior audit and MAS inspection findings.

6. **Risk-based audit coverage** – Annual audits should include key risk areas such as AML/CFT, technology risk and higher-risk business activities (e.g. DPT services, cross-border remittance and significant outsourcing arrangements).

7. **End-to-end review requirement for new PSPs or new services** – One year after commencing operations (or a new licensed service), end-to-end reviews of AML/CFT and technology risk controls should be conducted.

8. **Audit quality and remediation** – Auditors are expected to perform risk-targeted testing, while PSPs are expected to maintain evidence of remediation for previously identified deficiencies and regulatory findings.

PSPs should review their existing audit arrangements and regulatory compliance frameworks to ensure readiness for the enhanced audit expectations. Particular attention should be given to audit scope, regulatory reporting processes, safeguarding controls, AML/CFT compliance, technology risk management, outsourcing oversight and the tracking of remediation actions arising from audits and MAS inspections.

Please refer to the newly issued Guidelines at this link.

13 July 2026 – Information Paper on AML/CFT Supervisory Expectations for DPT

On 13 July 2026, the Monetary Authority of Singapore (MAS) issued an Information Paper on AML/CFT Supervisory Expectations for Digital Payment Token (DPT) Service Providers. The paper outlines MAS' supervisory observations and expected good practices following its inspections and supervisory engagements with DPT service providers.

This information paper sets out MAS' supervisory expectations in the areas of:

1. **Assessment of Risks Arising from New Products** - DPT service providers are expected to conduct robust risk assessments before launching new products, services, technologies or business initiatives to identify and mitigate potential money laundering, terrorism financing and proliferation financing risks.
2. **Enhanced Customer Due Diligence on Higher-Risk Customers** - MAS expects firms to apply enhanced due diligence measures to higher-risk customers, including obtaining additional information on the customer, source of wealth, source of funds and the purpose of the business relationship where appropriate.
3. **Value Transfer Requirements** - DPT service providers should have controls to comply with applicable value transfer requirements, including the collection, verification and transmission of required originator and beneficiary information where required.
4. **Ongoing Monitoring** - Firms are expected to implement effective transaction monitoring processes and ongoing reviews of customer profiles to ensure that transactions remain consistent with their understanding of the customer and the customer's risk profile.
5. **Screening** - MAS expects DPT service providers to maintain robust screening controls, including sanctions screening, adverse media screening and screening against relevant watchlists on a risk-sensitive basis.
6. **Due Diligence on Partners and Outsourced Service Providers** - Firms should conduct appropriate due diligence and ongoing oversight of business partners, intermediaries and outsourced service providers, particularly where such arrangements may impact the effectiveness of AML/CFT controls.
7. **Training and Staff Expertise** - DPT service providers should ensure that directors, senior management and staff receive adequate AML/CFT training and possess the necessary expertise to identify and manage emerging risks associated with digital payment token activities.

DPT service providers should review their AML/CFT frameworks against the supervisory expectations set out in the Information Paper, with particular focus on:

- New product approval and risk assessment processes;
- Enhanced due diligence procedures for high-risk customers;
- Compliance with value transfer requirements;
- Transaction monitoring and suspicious transaction reporting controls;
- Sanctions and adverse media screening frameworks;
- Oversight of outsourcing and third-party arrangements; and
- Staff competency, training and governance arrangements.

Please refer to the information paper at this link.

Hong Kong

SFC Circular on Robust Authentication and Monitoring Measures Against Phishing Attacks (9 July 2026)

On 9 July 2026, the SFC issued a circular requiring internet brokers and SFC-licensed virtual asset service providers (VASPs) to strengthen authentication, monitoring and incident response measures against phishing attacks. Senior management, particularly the Managers-in-Charge of Overall Management and Oversight (MIC of OMO) and Information Technology (MIC of IT), is ultimately responsible for implementing the enhancements and protecting client accounts.

Key Requirements

- Preventive Controls
  - Authentication – Implement phishing-resistant authentication for client logins as well as for device registration and binding. Email and SMS one-time passwords ("OTPs") are not regarded as phishing-resistant. Acceptable methods include passkeys and securely bound devices.
  - Risk-based selection – The firm should assess its specific circumstances, including the types and risk profile of its internet trading platforms, and adopt the authentication method proportionate to those risks.
  - Device / passkey limits – Clients should generally be limited to three registered passkeys and/or three bound devices. Additional registrations require adequate assessment. Existing clients with already-bound devices do not need to rebind.
  - Session controls – Clients should not be allowed to disable session timeouts. Idle sessions should generally be limited to 30 minutes unless a longer period is justified and closely monitored.
  - Ongoing review – The firm should stay abreast of technological developments relevant to its platform(s) and regularly reassess its security controls to ensure they remain appropriate.
- Detection
  - Client notifications – Promptly notify clients of successful logins and high-risk account activities, such as new-device logins, device binding, and the creation or revocation of passkeys.
  - Client-side reporting – Remind clients to inform the firm immediately of any suspicious account activity so that unauthorised actions can be addressed promptly.
  - Re-confirmation of material changes – Firms are strongly encouraged to require clients to confirm or acknowledge material account changes or unusual activities before permitting further transactions.
  - Transaction monitoring – Use predefined thresholds, based on the client's profile, past trading behaviour, account activity, device usage, and login patterns to detect abnormal trading. Red flags may include unusual trading patterns, multiple accounts linked to the same device, and transactions made shortly after account details are changed.
  - Login and device binding monitoring – Maintain adequate logs (including device IDs captured at login and device binding) and review them promptly. Irregular events to monitor include

binding requests from unusual locations, multiple accounts linked to the same device, logins from different locations within a short timeframe, and unusually prolonged login sessions.

- Incident Response and Reporting
  - Immediate response – Establish procedures to promptly respond to hacking incidents, including immediate measures to stop unauthorised activities, safeguard client assets, notify affected clients, and prevent further compromise.
  - Regulatory reporting – Report hacking incidents to the SFC immediately.
  - Root-cause analysis – Conduct a root-cause analysis to identify any internal control weaknesses or system vulnerabilities that led to the incident.
  - Documentation and remediation – Maintain comprehensive incident reports and implement appropriate remedial actions to strengthen controls and prevent recurrence.
- Client Awareness
  - Education – Inform clients of common attack scenarios and remind them never to share their login credentials with any third party under any circumstances.
  - Security reminders – Regularly encourage clients to follow sound security practices and to promptly review and report any suspicious or unauthorised account activity.

Implementation Timeline:

What	By When
Enhance monitoring, alerts and response procedures	Immediately
Boost client awareness	As soon as practicable
Roll out phishing-resistant authentication	By 8 July 2027 (12-month runway)
Large internet brokers	Immediately – no grace period

During the implementation period, firms continuing to use OTPs must enhance suspicious-activity monitoring and immediately suspend or restrict access where potentially fraudulent activity is identified.

Firms anticipating difficulty meeting the deadline must immediately notify their SFC case officer-in-charge.

The SFC may hold firms accountable for client losses where inadequate controls fail to prevent, detect or stop large-scale unauthorised transactions following hacking incidents.

If you have any questions regarding this circular or require assistance, please contact Waystone.

To view the circular, please click here.

Joint Circular on the Cross-Sectoral Cyber Mapping Exercise (29 July 2026)

On 29 July 2026, the HKMA, SFC, Insurance Authority and MPFA (collectively, the “Authorities”) issued a joint circular announcing the outcomes of the first production run of Hong Kong's cross-sectoral Cyber Mapping exercise, completed in March 2026. Supported by the Financial Services and the Treasury Bureau (FSTB) and aligned with the IMF's analytic framework and an FSAP recommendation, the initiative delivers a visual map of how over 50 financial institutions across banking, retail payment, securities, MPF and insurance are interconnected at both business and technology levels.

Why This Matters

As financial institutions increasingly use shared technologies, infrastructure and third-party service providers, a cyber incident at one key provider, such as a cloud provider or data centre, could affect many firms across the financial system. The Cyber Map helps regulators identify these concentration risks and interdependencies before they occur.

Key Findings from the First Run

- No “unknown-unknown” systemic risks – The largest nodes are the FIs, financial market infrastructures and major tech/data service providers already known to regulators.
- Certain third-party providers warrant closer supervisory attention – Common adoption patterns emerged around network infrastructure appliances, cybersecurity solutions (e.g., security event monitoring, privileged access management), and specialist vendors in payment processing and customer communications. This does not signal a systemic issue, but supports early, forward-looking monitoring.
- Cyber mapping is a valuable supervisory tool - Its dashboard-based design enables scenario-based filtering, supporting third-party risk supervision and incident triage. The Authorities may, in future, extend dashboard access to FIs for their own risk management.

What’s Next

- The Authorities will integrate the Cyber Map into day-to-day supervision, particularly for third-party risk and incident management.
- Where warranted, they may pursue drill exercises, thematic reviews and cross-sectoral contingency arrangements.
- The exercise will become a recurring fixture, with the next run expected in 2027/2028, featuring refined methodology, broader participant coverage and permanent infrastructure.
- Bilateral, confidential feedback will be shared with participating FIs.

If you have any questions regarding this circular or require assistance, please contact Waystone.

To view the circular, please click here.

Enforcement News – July 2026

SFC suspends former Yuanta representative for nine months (06 July 2026)

Summary of Facts

The SFC suspended Mr Wong Tim Hi, a former licensed representative of Yuanta Securities (Hong Kong) Company Limited, for nine months (from 3 July 2026 to 2 April 2027). The disciplinary action arose from the SFC's investigation into a market manipulation scheme involving shares of Ching Lee Holdings Limited.

Between June 2016 and May 2017, Wong:

- Allowed two third parties to become significantly involved in operating four client accounts without obtaining written authorisation from the clients
- Disclosed confidential account and transaction information, including fund movements and balances, to those third parties
- Failed to verify whether proper written authorisation was in place, despite being aware of the third party's significant involvement.

The SFC found that Wong breached Yuanta's internal policies, failed to protect clients' interests and called into question his fitness and properness to be licensed.

Key Takeaways

- Written client authorisation – Licensees must obtain and verify written client authorisation before allowing any third party to operate a client's account.
- Client confidentiality – Account details, transaction data or fund information must not be shared with unauthorised third parties.
- Wilful blindness is not a defence – Ignoring significant third-party involvement may lead to disciplinary action, even if the licensee is not involved in the underlying misconduct.
- Compliance with internal controls – Licensees should strictly follow internal account-handling procedures, properly document all third-party authorisations, and only disclose client account or transaction information with the client's express written consent.

To view the case, please click here.

SFC reprimands and fines Victory Securities Company Limited $1.7 million and suspends its Responsible Officer for regulatory breaches (24 July 2026)

Summary of Facts

The SFC reprimanded and fined Victory Securities Company Limited HK$1.7 million for regulatory breaches in handling a client account. It also suspended its Responsible Officer and Manager-in-Charge, Mr. Stephen Chiu Che Leung, for three months (from 22 July 2026 to 21 October 2026).

The case arose from the SFC's investigation into a suspected ramp-and-dump scheme. In October 2019, a client opened an account at Victory to sell shares purportedly held at another brokerage, supported by statements provided by the client.

The SFC found that Victory:

- Failed to make adequate enquiries before executing the client's sale orders, despite multiple red flags
- Failed to properly assess whether the client's declared shareholding was proportionate to his financial profile
- Failed to follow up properly when subsequent information suggested that the client may have provided false documents
- Failed to report the suspected fraudulent conduct to the SFC.

The SFC found Victory's conduct fell short of the Code of Conduct, the AMLO and the AML/CFT Guideline. The failures were also attributed to Mr. Chiu's neglect of his supervisory duties.

Key Takeaways

- Robust internal controls – Firms should ensure their KYC, AML and transaction monitoring controls are robust enough to identify and escalate inconsistencies between a client's profile and trading activity.
- Senior management accountability – ROs and MICs may be personally liable for supervisory failures, even in isolated incidents.

To view the case, please click here.

SFC reprimands and fines Bright Smart Securities International (H.K.) Limited $2.8 million for internal control failures in monitoring suspicious trades (27 July 2026)

Summary of Facts

The SFC reprimanded and fined Bright Smart Securities International (H.K.) Limited (BSSIHK) HK$2.8 million for inadequate controls to detect and prevent client wash trades. Between 1 November 2023 and 13 September 2025, BSSIHK allowed 1,021 pairs of wash trades involving 736 stocks and warrants across 615 client accounts.

The SFC found that BSSIHK:

- Relied mainly on post-trade monitoring and manual reviews before March 2024, meaning wash trades could be executed before detection
- Introduced a pre-trade interception arrangement in March 2024, but the arrangement remained inadequate
- Depended on manual intervention rather than fully automated pre-trade controls

- Failed to properly identify repeated misconduct, including multiple same-day wash trades in the same account.

The SFC also noted that BSSIHK had previously been reminded to strengthen its controls but failed to fully address the issues.

Key Takeaways

- Appropriate trade monitoring – Firms should maintain robust, automated, and properly calibrated trade surveillance systems to detect and prevent wash trades before execution.
- Testing of controls – Firms should regularly review and test their surveillance frameworks to ensure thresholds, triggers, and escalation procedures effectively capture repeated misconduct, including multiple same-day incidents.
- Effective remediation – Any deficiencies identified by the SFC should be addressed promptly and fully.

To view the case, please click here.

SFC fines China Industrial Securities International Asset Management for private fund failures (27 July 2026)

Summary of Facts

The SFC reprimanded and fined China Industrial Securities International Asset Management Limited (CISIAM) HK$6.8 million for failures in managing a private fund for Tahoe Life Insurance Company Limited between August 2019 and September 2020.

The case involved complex investment arrangements entered into by CISIAM for the fund, including structured notes linked to debt instruments issued by Tahoe Life's related company.

The SFC found that the arrangements:

- Lacked a clear commercial rationale
- Created additional risks and costs
- Raised concerns over possible concealment of asset movements or connected party transactions.

Despite these red flags, CISIAM failed to:

- Exercise independent judgment
- Conduct proper due diligence
- Ensure compliance with the fund's investment restrictions and objectives
- Maintain effective risk controls.

For further details, please refer to the article prepared by Waystone.

To view the case, please click here.

SFC fines Luk Fook Securities HK$2.1 million over cybersecurity failures (28 July 2026)

Summary of Facts

The SFC reprimanded and fined Luk Fook Securities (HK) Limited (LFSHK) HK$2.1 million for inadequate cybersecurity controls following a ransomware attack on 19 September 2022.

The attack disrupted LFSHK's key systems, including:

- Trading systems
- Email servers
- Accounting servers
- File servers

As a result, clients were unable to trade via the mobile app or internet platform until systems were restored in phases by 7 October 2022.

The SFC found multiple control failures, including:

- Inadequate firewall protection and network monitoring
- Outdated operating systems and antivirus software
- Weak user access and password controls
- Insecure storage of credentials
- Insufficient controls over remote access and external devices
- Lack of regular cybersecurity training
- Inadequate data backup and business continuity arrangements.

Key Takeaways

Robust cybersecurity controls – Licensed corporations should maintain effective cybersecurity controls across all critical systems, including firewall protection, network monitoring, system patching, antivirus protection, secure remote access, and external device controls.

Strong access and password management – Firms should implement proper user access controls, privileged account management, password policies, and secure storage of credentials.

Cybersecurity training and resilience – Firms should provide regular cybersecurity awareness training and maintain tested data backup and business continuity plans.

Regulatory accountability – Disciplinary action may follow even where no direct client loss occurs.

To view the case, 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 →