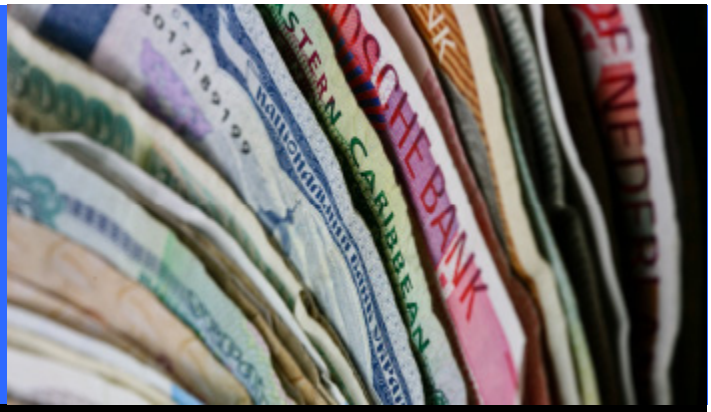
View on our website.

GIBSON DUNN




**Financial Regulatory Update** June 12, 2026

# Hong Kong Updates Guidance on Provision of Custodial Services for Digital Assets by Authorized Institutions

*The Updated Guidance applies to AIs providing custodial services for digital assets, defined broadly to include virtual assets, tokenized securities and other tokenized assets. It does not apply to the custody of proprietary assets held by AIs or their group companies which are not held on behalf of clients.*

On 27 May 2026, the Hong Kong Monetary Authority (**HKMA**) published updated guidance on the expected standards for the provision of custodial services for digital assets by authorized institutions (**AIs**) (**Updated Guidance**).[1] The Updated Guidance supersedes and substantially expands the HKMA's original guidance issued on 20 February 2024 (**Guidance**).[2]

The revisions reflect the HKMA's assessment of emerging risks in the digital asset custody space, including the evolving cyber threat landscape, lessons drawn from significant industry incidents, and the rapid expansion of the digital asset ecosystem since the Guidance was originally issued. This client alert sets out the key changes introduced in the Updated Guidance.

The Updated Guidance applies to AIs providing custodial services for digital assets, defined broadly to include virtual assets (**VAs**), tokenized securities and other tokenized assets. It does not apply to the custody of proprietary assets held by AIs or their group companies which are not held on behalf of clients.

## I. Governance and Risk Management Requirements

The Updated Guidance contains two notable amendments to the HKMA's requirements in relation to the governance and risk management:

- The Updated Guidance introduces a new training requirement specifically for transaction signers, who must now receive comprehensive training to ensure that they fully understand verification requirements and the appropriate handling procedures for exception or uncertainty concerning a transaction.
- AIs are already required to establish and maintain effective contingency and disasters recovery arrangements to ensure business continuity of its custodial activities. The Updated Guidance clarifies that AIs should also conduct drills to address emergency and business continuity plan (**BCP**) scenarios.

## II. Technical Safeguarding Controls

The most significant changes in the Updated Guidance relate to the technical requirements for safeguarding client digital assets. In particular, the Updated Guidance requires AIs to have written policies and procedures for the below measures:

- **Detecting unauthorized access and transactions**: In addition to existing obligations regarding access controls and authentication, the Updated Guidance requires AIs to establish a robust mechanism to detect unauthorized access or intrusions to critical wallet infrastructure, including cold wallet vaults, signing devices, databases, production binaries and code repositories. AIs are also expected to establish robust systematic controls to prevent unauthorized transactions from cold wallets. This includes introducing whitelist controls to prevent asset transfer to unapproved wallet addresses and stringent controls on changes to the cold wallet whitelists. Each transaction must also be subject to systematic verification to ensure authorization.
- **Handling of security incidents**: When responding to security alerts and incidents, AIs should classify them based on severity levels and apply corresponding response protocols accordingly.

The HKMA's original Guidance emphasized that AIs are expected to adopt industry best practices and follow applicable international security standards in a way that is commensurate with the nature, features and risks of the assets being held, but also set out a range of procedures and controls that the HKMA generally expected AIs to adopt in relation to holding of client VAs. The Updated Guidance expands this list of procedures and controls as follows:

- **Hardware Security Module (HSM) due diligence**: The Updated Guidance introduces new requirements in respect of HSMs. AIs must now (i) perform appropriate due diligence on the HSM provider before onboarding, and (ii) conduct periodic ongoing evaluations to ensure the vendor maintains security standards through effective patch management, and that any patched HSM is validated and its certification updated promptly.
- **Localization of seeds and private keys**: The Updated Guidance retains the requirement to securely generate, store and back up seeds and private keys in Hong Kong. However, there is a limited exception for HKMA-licensed stablecoin issuers – with the HKMA's consent, such an issuer may be appointed by an AI (e.g. under a delegation or

outsourcing arrangement) to provide custody services for specified stablecoins it issues, provided the seeds and/or private keys are safeguarded and backed up in Hong Kong or a location acceptable to the HKMA. This reflects the new stablecoin regulatory framework introduced under the Stablecoins Ordinance (Cap. 656).[3]

- **Cold wallet architecture requirement**: The Updated Guidance introduces two new requirements specific to cold wallet architecture. First, cold wallet implementations must not include smart contracts on public blockchains, in order to minimize potential online attack vectors associated with on-chain smart contracts. Second, in client cold wallet operations, devices used for transaction approval must now be dedicated, with restricted functionality and limited network connectivity, and must be isolated from general purpose workstations. Critically, integrity checks on critical transaction data must be conducted using air-gapped devices stored in a cold vault, which require physical access for code modifications.

- **Assessment of potential attack vectors**: The Updated Guidance requires AIs to assess potential attack vectors on a regular basis, including before any material changes to processes, systems or authorized personnel, and to implement multiple layers of independent data integrity checks across the transaction lifecycle with an end-to-end integrity protection and proper segregation of duties.

- **Segregation of duties**: Segregation of duties and comprehensive oversight mechanisms must be strictly enforced for wallet system code management, whether the codebase is developed internally or externally. These controls should encompass gatekeeping procedures such as code reviews, testing, software supply chain management, approvals and secure deployment practices, all of which should be supported by comprehensive audit trails. Administrator access to production systems must adhere to the principles of least privilege and privilege separation as well as industry best practices.

- **Anti-blind signing controls**: The Updated Guidance introduces a new requirement to prevent blind signing (i.e., the practice of signing a transaction without being able to view and verify its details). AIs must implement robust measures to prevent blind signing and ensure effective manual transaction review or approval. All details of a transaction requiring manual review must be displayed in a clear, human-readable format to allow signers to review before signing.

- **Third party transfers**: The Updated Guidance relaxes the prior absolute restriction on transfers to non-client wallet addresses. Under the Updated Guidance, deposits and withdrawals of client digital assets need only be made through whitelisted wallet addresses belonging to clients, except for transfers to support payment services or to execute client settlement instructions, where third-party transfers will be permitted, provided that effective risk controls are in place.

- **Revised insurance requirements**: The Guidance included a requirement for AIs to maintain a compensation or insurance arrangement covering potential losses of at least 50% of client digital assets in cold storage and 100% of client digital assets in hot and other storage. Importantly, this prescriptive insurance floor has been removed in the Updated Guidance. In its place, the Updated Guidance provides that AIs must be liable to their clients for the loss of any client digital assets arising in relation to an incident attributable to the AI and must ensure that they have adequate financial resources, which "may include" suitable insurance arrangements to cover potential losses. We anticipate that this will be favourably received by the industry, as the previous compensation / insurance requirements had been considered by many to be onerous to comply with.

## III. Delegation and Outsourcing Obligations

The Updated Guidance expands the list of permissible delegees for VA custody functions. Under the Guidance, AIs could only delegate or outsource VA custody to (i) another AI (or subsidiary of a locally incorporated AI), or (ii) a VA trading platform licensed by the Securities and Futures Commission (**SFC**). The Updated Guidance adds a third category: an HKMA-licensed stablecoin issuer that has obtained the HKMA's consent to provide custody for specified stablecoins it issues, provided the issue of such stablecoins is authorized under the Stablecoins Ordinance.

The Updated Guidance further significantly expands the ongoing monitoring obligations for delegation and outsourcing arrangements. Under the Guidance, AIs were required to monitor and review the performance of delegates and service providers on an ongoing basis. The Updated Guidance retains this obligation but adds prescriptive detail as to what that monitoring must entail:

- regular evaluation of the delegate's or service provider's security controls and operational processes;
- mandatory timely reporting of incidents and emerging risks;
- regular testing of the delegate's or service provider's disaster recovery capabilities;
- regular inherent risk assessments covering third-party dependencies and vulnerability management, with mitigation measures to address residual risks;
- periodic independent cybersecurity assessments of the deployed systems; and
- regular end-to-end rehearsals to ensure that business continuity plans meet recovery time objectives.

## IV. Ongoing Monitoring Framework

The Updated Guidance enhances existing ongoing monitoring obligations as follows:

- Any system changes, including the implementation of new systems or upgrades to existing ones, must undergo thorough testing prior to deployment. Security monitoring should be conducted on a 24/7 basis, supported by adequate resourcing and established procedures to address contingencies and incidents at any time, including during holidays.
- The Updated Guidance clarifies that monitoring processes must extend beyond the custody system itself to encompass its dependencies, including vendors, technologies, blockchain protocols, encryption algorithms and common libraries that may impact the safety of client assets.
- The monitoring framework must also incorporate consideration of significant industry incidents and publicly identified security vulnerabilities that may threaten the integrity of the custody system and related components. In practice, this requires AIs to maintain an active awareness of the broader digital asset security landscape and to undertake ongoing assessments regarding the relevance of industry incidents to their own systems and controls.

## V. Anti-Money Laundering and Counter-Financing of Terrorism

You may notice that the Updated Guidance drops the original Guidance's standalone Anti-Money Laundering and Counter-Financing of Terrorism (**AML/CFT**) section, which required AIs to manage the money laundering and terrorist financing risks of their custodial activities and to comply with the HKMA's Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) (**AML/CFT Guideline**).[4] However, this should not be interpreted as a relaxation. That section merely cross-referred to obligations imposed elsewhere, and AIs remain fully subject to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)[5] and the HKMA's AML/CFT Guideline. This is reinforced by the covering circular's reminder that AIs must comply with all applicable legal and regulatory requirements. As such the purpose of the deletion appears to be to avoid duplicating requirements for the dedicated AML/CFT framework, rather than to change what is expected of AIs.

## VI. Provision of Staking Services

Finally, the Updated Guidance draws attention to HKMA guidance on staking services issued on 7 April 2025, which mandates AIs providing VA staking services from custodial arrangements to implement robust internal controls to safeguard client assets, retain control over unstaking mechanisms, and manage operational and conflict risks.[6] The Updated Guidance also reminds AIs that, in complying with the relevant requirements, they should also have due regard to the terms and conditions for providing staking services as imposed by the SFC on SFC-licensed VA trading platforms.[7]

## VII. Conclusion

While the HKMA's Updated Guidance applies only to AIs, it contains important indications regarding the direction of travel for Hong Kong's broader VA ecosystem. In particular, many of the requirements set out in the Updated Guidance, such as robust segregation of client assets, stringent governance over private key management, monitoring of delegation and outsourcing – are broadly consistent with the policy trajectory already outlined by the Securities and Futures Commission (SFC) in relation to custody of virtual assets.[8] Given this, we anticipate that many of the requirements in the Updated Guidance will also form part of the detailed regulatory requirements imposed on licensed VA custodian service providers under the SFC's forthcoming VA custody regime.

Additionally, in light of the significant changes introduced by the Updated Guidance, AIs providing or contemplating digital asset custodial services should consider conducting a review of their internal systems and controls against the enhanced requirements under the Updated Guidance to identify and remediate any gaps.

[1] "*Updated Guidance on Expected Standards on Provision of Custodial Services for Digital Assets by Authorized Institutions*" published by the Hong Kong Monetary Authority on 27 May 2026, accessible here.

[2] "*Guidance on Expected Standards on Provision of Custodial Services for Digital Assets by Authorized Institutions*" published by the Hong Kong Monetary Authority on 20 February 2024, accessible here.

[3] Stablecoins Ordinance (Cap. 656), accessible at: https://www.elegislation.gov.hk/hk/cap656. See also "*Hong Kong Gets Ready for Stablecoin Regulation: HKMA Prepares for Enactment of the Regime*" published by Gibson, Dunn & Crutcher on 4 June 2025, accessible at: https://www.gibsondunn.com/hong-kong-gets-ready-for-stablecoin-regulation-hkma-prepares-for-enactment-of-the-regime/.

[4] "*Guideline on Anti-Money Laundering and Counter Financing of Terrorism (For Authorized Institutions)*" published by the Hong Kong Monetary Authority on May 2023, accessible at: https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20230525-4-EN/AML-2.pdf.

[5] Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615), accessible at: https://www.elegislation.gov.hk/hk/cap615.

[6] "*Provision of Staking Services for Virtual Assets from Custodial Services*" published by the Hong Kong Monetary Authority on 7 April 2025, accessible at: https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20250407-1-EN/20250407-1-EN.pdf.

[7] "Terms and conditions for providing staking services" published by the Securities and Futures Commission on 7 April 2025, accessible here.

[8] See, for example, "*Circular to licensed virtual asset trading platform operators on custody of virtual assets*" published by the Securities and Futures Commission, accessible here.

**The following Gibson Dunn lawyers prepared this update: William Hallatt, Emily Rumble, and Jane Lu.**

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. If you wish to discuss any of the matters set out above, please contact any member of Gibson Dunn's Financial Regulatory team, including the following members in Hong Kong:

William R. Hallatt (+852 2214 3836, whallatt@gibsondunn.com)

Emily Rumble (+852 2214 3839, erumble@gibsondunn.com)

Arnold Pun (+852 2214 3838, apun@gibsondunn.com)

Becky Chung (+852 2214 3837, bchung@gibsondunn.com)

Jane Lu (+852 2214 3735, jlu@gibsondunn.com)