

Client alert:

HKMA digital assets custody guidance for Authorized Institutions (AIs)

Executive summary

On 20 February 2024, the Hong Kong Monetary Authority (HKMA) released a comprehensive and timely circular (the Circular) pertaining to the custody of digital assets (DAs) held on behalf of clients by Authorized Institutions (AIs). Since DAs cover not only virtual assets (VAs) but also (1) tokenised securities and (2) other tokenised assets, the Circular is of high relevance to a wide variety of tokenisation initiatives being undertaken by AIs. It is also relevant to the custody of spot VA ETFs (for a more lengthy analysis of the ETF regime for VAs, please refer to the most recent PwC client alerts on VA ETFs [here](#) and [here](#)).

This client alert outlines the new DA custody requirements in Hong Kong and provides some highlights regarding how AIs can continue operating in compliance with the Banking Ordinance (Cap. 155) when venturing into DA custody.

Background

Whilst the regulatory framework for digital assets is steadily strengthening in Hong Kong, there is currently no standalone framework dedicated to digital asset custody.

Currently, VA custodians in Hong Kong only need a Trust or Company Service Providers (TCSP) Licence under the city's Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) to operate (as long as they do not act as trustees, or engage in over-the-counter trading activities).

Taking a step back, the current situation contrasts with the regulatory clarity that Hong Kong regulators have been increasingly providing to the DA ecosystem. It also contrasts with how seriously institutional participants take custody when considering any asset class (and even more so DAs for a variety of reasons including the non-reversible nature of some DA transactions).

The HKMA has therefore outlined a series of requirements for the custodial activities of AIs, that now open the possibility for HKMA regulated AIs to provide such services.

Application of the Circular

Under the Circular, custodial activities are widely scoped and cover more than just the provisioning of standalone custodial services. In fact, those would include custody activities as they relate to the distribution of tokenised products. For Hong Kong locally incorporated AIs, the rules also apply to their subsidiaries.

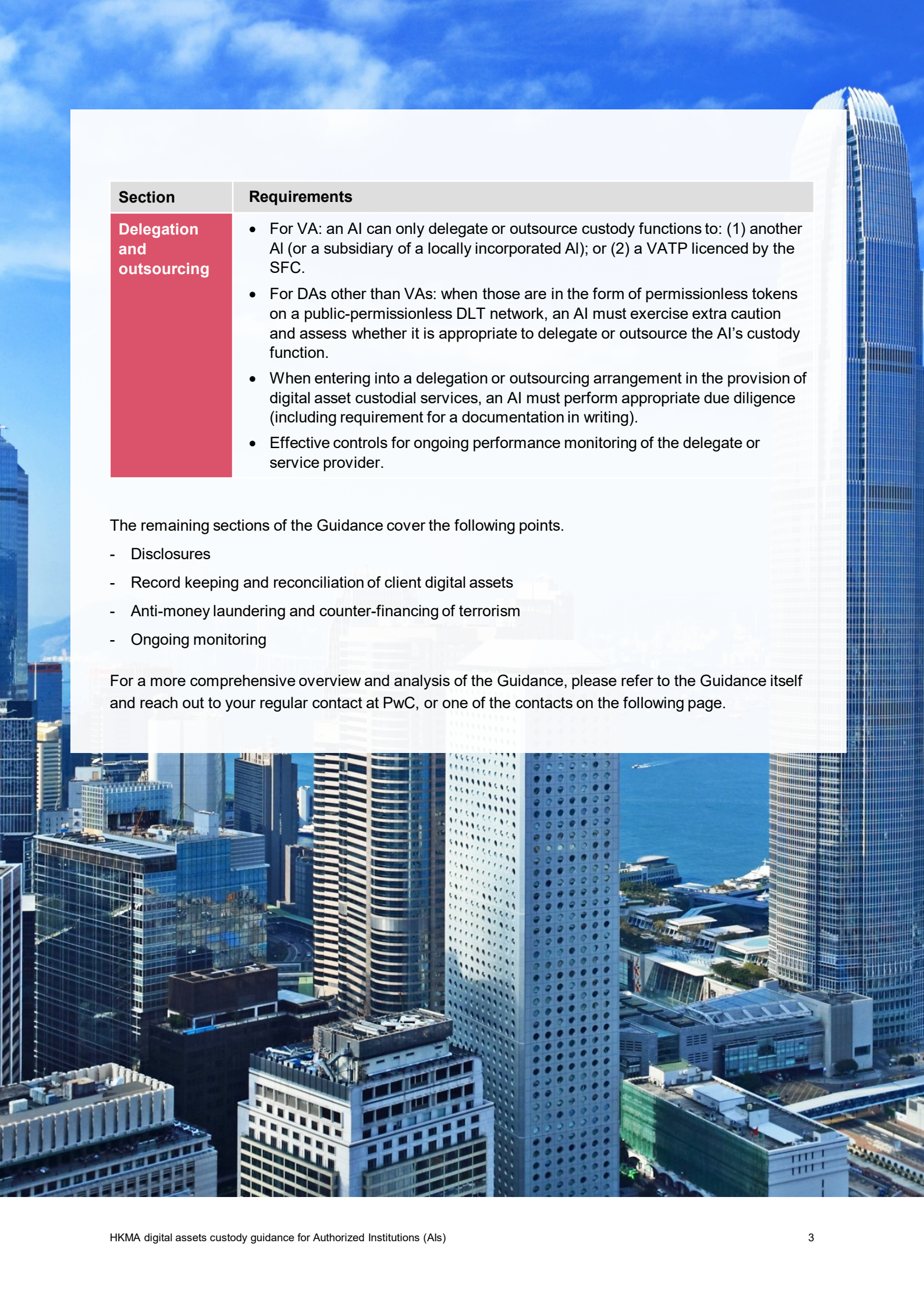
Additional points to note (a more detailed summary is provided in below table):

- VAs and the rest of DAs are distinguished and higher standards are applied to the custody of VAs (relative to those for other DAs).
- The nature of the blockchain (permissionless or not) on which DAs exist makes a difference regarding the security measures the AI is required to implement.
- The requirements in the Circular are largely consistent with the SFC's Virtual Asset Trading Platform (VATP) Guidelines save for a few areas.
- Most of the Guidance focuses on due diligence, governance and controls, risk disclosures and risk management.

High level requirements

The following table provides some highlights of the standards set by the Circular.

Section	Requirements
Governance and risk management	<ul style="list-style-type: none">• Comprehensive risk assessment to identify and understand risks.• Effective Board and senior management oversight, adequate resources, including personnel and expertise, to ensure proper governance, operations and effective risk management.• Adequate policies and processes to identify, manage and mitigate potential and/or actual conflicts of interest.• Effective contingency and disaster recovery arrangements to ensure business continuity of custodial activities.
Segregation of client digital assets	<ul style="list-style-type: none">• Hold client digital assets in separate client accounts segregated from the AI's own assets.• Not transfer any right, interest, ownership, legal and/or beneficial title in client digital assets or otherwise lend, pledge, repledge or create any encumbrance over client digital assets, except on some specified circumstances.• Adequate and effective measures to prevent the use of client digital assets for the AI's own account or for purposes other than those agreed with its clients.
Safeguarding of client digital assets	<ul style="list-style-type: none">• Systems and controls to safeguard client digital assets to include, among others, written policies and procedures for (1) authorising and validating access to effecting deposit, withdrawal and transfer of client digital assets, including the access to the devices storing seeds and private keys; and (2) managing and safeguarding seeds and private keys of client digital assets, covering key generation, distribution, storage, use, destruction and backup.• Localisation expectations in relation to private keys.• Effective client authentication and notification controls for any user interface or portal for clients to manage digital assets.



Section	Requirements
Delegation and outsourcing	<ul style="list-style-type: none">• For VA: an AI can only delegate or outsource custody functions to: (1) another AI (or a subsidiary of a locally incorporated AI); or (2) a VATP licenced by the SFC.• For DAs other than VAs: when those are in the form of permissionless tokens on a public-permissionless DLT network, an AI must exercise extra caution and assess whether it is appropriate to delegate or outsource the AI's custody function.• When entering into a delegation or outsourcing arrangement in the provision of digital asset custodial services, an AI must perform appropriate due diligence (including requirement for a documentation in writing).• Effective controls for ongoing performance monitoring of the delegate or service provider.

The remaining sections of the Guidance cover the following points.

- Disclosures
- Record keeping and reconciliation of client digital assets
- Anti-money laundering and counter-financing of terrorism
- Ongoing monitoring

For a more comprehensive overview and analysis of the Guidance, please refer to the Guidance itself and reach out to your regular contact at PwC, or one of the contacts on the following page.

Contact us



Duncan Fitzgerald
Financial Services
Risk Assurance Leader
PwC Hong Kong
+852 2289 1190
duncan.fitzgeralds@hk.pwc.com



James Tam
Banking and Capital Markets
Leader
PwC Hong Kong
+852 2289 2706
james.tam@hk.pwc.com



Peter Brewin
Crypto and Web3 Co-Leader,
Tax Partner
PwC Hong Kong
+852 2289 3650
p.brewin@hk.pwc.com



Henry Cheng
Senior Advisor
PwC Hong Kong
+852 2289 8208
henry.f.cheng@hk.pwc.com



Lei Wang
Risk Assurance Partner
PwC Hong Kong
+852 2289 1921
lei.l.wang@hk.pwc.com



Michael Footman
Financial Services
Risk and Regulation Leader
PwC Hong Kong
+852 2289 2747
michael.hc.footman@hk.pwc.com



Adrian Clevenot
Associate Director
PwC Hong Kong
+852 2289 5522
adrian.a.clevenot@hk.pwc.com



Gary Ng
Partner
PwC Hong Kong
+852 2289 2967
gary.ng@hk.pwc.com