



DIGITAL ASSETS SERIES: CHAPTER 3

LEGAL UPDATE
BY KHAILING YAU CHAMBERS
2021

Chapter 3: Digital Asset Custodian (“DAC”) and the Regulatory Framework for DACs in Malaysia

In this Chapter 3 of our Digital Assets Series, we consider the regulatory framework for digital asset custodians in Malaysia.

1. Digital Asset Custodian

1.1 Introduction

- (a) Under the [Guidelines on Digital Assets](#) (“**DA Guidelines**”), the obligations of an initial exchange offering (“**IEO**”) operator in relation to the investors’ digital tokens are to:
- (i) ensure that the token holders’ digital tokens are properly segregated and safeguarded from conversion or inappropriate use by any person;
 - (ii) establish and maintain a sufficiently and verifiably secured storage medium designated to store digital assets from investors; and
 - (iii) establish system and controls for maintaining accurate and up-to-date records of client’s digital assets held.
- (b) To carry out such obligations, an IEO operator may appoint a DAC registered with the Securities Commission Malaysia (“**SC**”) to provide custody for the token holders’ digital tokens, or it can choose to provide its own custody services, provided it complies with the requirements set out under Part D of the DA Guidelines. In essence, an IEO operator who wishes to provide custody for the token holders’ digital tokens has to, in addition to being registered as an IEO operator, has to be registered with the SC as a DAC as well.
- (c) The DA Guidelines define a DAC as a person who provides services such as safekeeping, storing, holding or maintaining custody of digital assets for the account of another person, and such services constitute capital market services for the purposes of Section 76A of the CMSA. Hence, a prospective DAC must satisfy all the requirements set out in Part D of the DA Guidelines and be registered by the SC.

1.2 Our Key Observation – The Control Element

Although the DA Guidelines do not specify the details or processes in which a DAC is to provide its custody services, it has explicitly stipulated that a person who merely offers a system by whatever means, which enables an asset owner to hold the digital assets, and the asset owner has full control over his digital assets, is **not** deemed to be a DAC for the purposes of the DA Guidelines. The DA Guidelines further elaborates that an asset owner

is considered to have “full control” over his digital assets when he holds the private key(s) to his wallet and the DAC does not have the ability to unilaterally transfer the digital assets. This indicates that for the DA Guidelines to apply, a DAC must have a substantial degree of control over the token holders’ digital tokens, for instance, having the ability to transfer the digital asset unilaterally.

1.3 Eligibility and registration requirements for DAC

<p>Type of entity</p>	<p>(a) Either a local or foreign entity.</p> <p>(b) In the case of an applicant who is a foreign entity, the SC must be satisfied that:</p> <ul style="list-style-type: none"> (i) the applicant is authorised to operate or carry out an activity of a similar nature in the foreign jurisdiction; (ii) the applicant is from a comparable jurisdiction with whom the SC has regulatory arrangements on enforcement, supervision and sharing of information; and (iii) it is in the best interest of Malaysia to register the foreign DAC. <p>(c) In determining “best interest of Malaysia”, the SC will take into account the following factors:</p> <ul style="list-style-type: none"> (i) the area of specialisation and level of expertise that can be offered to the capital market including the effect on productivity, transference of skills and efficiency and quality of capital market services; (ii) the risk posed on the systemic stability of the capital market including activities and conduct that will likely impact the orderly functioning of the capital market; (iii) the contribution towards attracting investments, enhancing market linkages and promoting vibrancy in the capital market; (iv) the ability in developing strategic or nascent sectors in the capital market; or (v) the degree and significance of participation of Malaysians in the capital market.
<p>Existing recognized market operator or registered trustee</p>	<p>Existing registered recognized market operators and registered trustees who seek to become a registered DAC are required to notify the SC of such intention, upon which the SC may carry out an assessment on the registered recognized market operator or registered trustee to determine whether it is able to satisfactorily</p>

	comply with the requirements under Part D of the DA Guidelines before deeming it to be a registered DAC.
Financial requirements	<p>Minimum:</p> <p>(a) paid-up capital of RM500,000; and</p> <p>(b) shareholders' funds of RM500,000 maintained at all times.</p>
Criteria for registration	<p>An applicant may be registered as a DAC if the SC is satisfied that all the following requirements are fulfilled:</p> <p>(a) the applicant, its directors, controller and senior management are fit and proper;</p> <p>(b) the applicant will be able to carry out its obligations as set out under the DA Guidelines;</p> <p>(c) the applicant will appoint at least one (1) responsible person;</p> <p>(d) the applicant will be able to manage risks associated with its business and operation including demonstrating the processes and contingency arrangement in the event the applicant is unable to carry out its operations;</p> <p>(e) the applicant has sufficient financial, human and other resources for its operation at all times; and</p> <p>(f) the applicant has appropriate security arrangements, taking into account the scale of its business operations and risks, which include maintaining a secured environment pursuant to the guidelines issued by the SC for the management of cyber risk and other relevant guidelines.</p>

1.4 Directors, Senior Management and Responsible Person

Directors and Senior Management	Directors, controller and senior management of the DAC must be fit and proper and are suitably qualified.
Responsible Person	<p>(a) A DAC must have at least one (1) responsible person ("Responsible Person") at all times who must be appointed from its senior management, and shall be the main contact person to liaise with the SC and to perform any duty as may be directed by the SC.</p> <p>(b) The Responsible Person must have a minimum five (5) years' of relevant industry experience or expertise and must be a fit and proper person.</p>

1.5 Obligations of a DAC

Obligations	<p>A DAC must, among others:</p> <ul style="list-style-type: none"> (a) act in the best interest of the clients and take all reasonable measures to avoid situations that are likely to involve conflict of interest with the clients; (b) safeguard the rights and interests of its clients including ensuring that its clients have access to their digital assets at all times, and preventing unauthorised access to clients' digital assets; (c) identify and manage risks associated with its business and operations, including having in place an effective business continuity plan; (d) establish and maintain written policies and procedures to, among others, ensure compliance with all relevant laws, regulations and guidelines including the Anti-Money Laundering and Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 and Personal Data Protection Act 2010; (e) ensure that its processes and practices are continuously aligned to industry practices in relation to custody of digital assets; (f) identify and manage potential vulnerabilities, cyber threats in its operating environment; (g) in the event of any systems error, failure or malfunction, take all necessary and immediate appropriate actions to mitigate any potential losses; and (h) carry out any other duties or responsibilities as may be specified by the SC.
--------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.6 Safeguard measures and ring-fence arrangements

Risk management	<p>A DAC must:</p> <ul style="list-style-type: none"> (a) establish a risk management framework to identify, assess, monitor, control and report all material risks to which it could be exposed to; and (b) carry out periodic reviews, audits and testing on systems, operational policies, procedures, and controls relating to risk management and its business continuity plan.
------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Conflict of interest management	A DAC must give priority to the clients' interest if there is a conflict between the clients' interests and its own interests.
Internal audit	A DAC must perform internal audit checks on its operations regularly.
Key generation and management	<p>A DAC must:</p> <ul style="list-style-type: none"> (a) establish and maintain a sufficiently and verifiably secured storage medium designated to store its clients' digital assets; (b) have in place effective policies and procedures to safeguard key generation and management including: <ul style="list-style-type: none"> (i) adopting industry standards and practices in terms of key generation and management; (ii) ensuring that its employees that are involved in the key generation process are identified and prevented from having unauthorised access to clients' digital assets; and (iii) having in place procedures to enable the clients to access their digital assets in the event the client loses his access credentials or where the keys have been compromised. (c) have in place effective security mechanisms for the digital assets including adopting measures such as having multi-factor authentication requirements before effecting any transaction on behalf of the clients.
Segregation of client assets	<p>The DAC must:</p> <ul style="list-style-type: none"> (a) ensure that all clients' digital assets are properly segregated from its own assets and safeguarded from conversion or inappropriate use by any person; and (b) establish system and controls for maintaining accurate and up-to-date records of clients' digital assets held.
Transaction handling	<p>The DAC must:</p> <ul style="list-style-type: none"> (a) ensure that, at all times, it has up-to-date transactional records relating to the clients' digital assets; (b) provide the information under (a) above to the SC as and when requested by the SC and in such form and manner as the SC may specify; and (c) retain all such transactional records for a minimum period of seven (7) years.

Outsourcing	<p>(a) Save for any function that involves:</p> <ul style="list-style-type: none"> (i) the decision-making functions of the DAC; or (ii) any interaction or direct contact with the clients, <p>all other functions of the DAC can be outsourced subject to the requirements of the DA Guidelines.</p> <p>(b) The board of directors of the DAC remains accountable for all outsourced functions.</p>
--------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.7 Changes requiring the SC's prior approval / notification to SC

Change in shareholding	A DAC must obtain the SC's prior approval if any proposed change to its shareholding will result in a direct or indirect change in its controller.
Additional classes of digital assets	A DAC must notify the SC in the event it intends to provide custodial services for additional classes of digital assets.

1.8 Cessation of business or operations

Prior engagement with the SC	A DAC shall not cease its business or operations without prior engagement with the SC and such cessation will not take effect until the SC is satisfied that all the requirements stated in the securities laws, the DA Guidelines, relevant guidelines issued by the SC and any other relevant laws or requirements have been fulfilled.
Direction by the SC	To ensure an orderly cessation of the business or operations of the DAC, the SC may issue a direction or impose any term or condition.
Uninterrupted access to digital assets	The DAC must ensure that its clients continue to have uninterrupted access to their respective digital assets under its custody in the event it ceases to operate or cannot fulfil its obligation under the custodial agreement.

1.9 Powers of the SC

Additional requirements	<p>The SC may at any time:</p> <ul style="list-style-type: none"> (a) impose additional financial requirements; and / or (b) vary, add or remove any requirements or terms and conditions on a DAC,
--------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	that commensurate with the nature, operations and risks posed by the DAC.
Directions	The SC may issue a direction to the DAC, its board of directors, any of its directors, senior management or any other person, if the SC is satisfied that it is necessary or expedient for the protection of the clients, or in the public interest.
Periodic assessment	The SC may conduct periodic assessment of a DAC's compliance with any or all of its regulatory obligations, and request documents or other assistance as required.
Powers under securities laws	In addition to the above, the SC shall also be entitled to exercise its powers under securities laws.

2. Our Observations: Potential Digital Asset Custody Models

2.1 Applications to the SC to be registered as a DAC commenced on 28 October 2020. As at the date of publication of this Article, the assessment process by the SC appears to be ongoing and we understand that no DAC has been registered by the SC. It therefore remains to be seen as to how a DAC is expected to undertake its role to provide digital asset custody services within the requirements of the DA Guidelines.

2.2 In general, digital asset custody may be structured differently depending on the profile, types of digital assets and requirements of the digital asset holders. For discussion purposes, we believe the structure of digital asset custody may be generally described as follows:

- (a) Self-custody
- (b) Partial custody
- (c) Third-party custody

2.3 Certain examples of how digital asset custody may be structured:

Type	Characteristics
Self-custody	<ul style="list-style-type: none"> • The digital asset owner has complete control of their private keys and digital assets. • No third-party involved to manage the risk or the funds in the event the digital asset owner loses access to private keys, experiences a destructive event such as a fire or power outage, or passes away unexpectedly. • The digital asset owner would need to consider factors such as their access to software updates, their personal capacity to correctly backup, restore and implement geographic redundancy, and how

Type	Characteristics
	<p>family members or intended beneficiaries would recover funds in emergency situations.</p>
<p>Partial custody</p>	<ul style="list-style-type: none"> • Self-managed wallet with third-party assistance and related institutional controls or protections. • Such an option may align the needs of certain retail or high-net-worth investors who want to control their holdings, but also desire some level of assurance and institutional protections shy of full third-party management. • Applies two-factor authentication or other identity verifications and/or basic multi-signature protection where the DAC possesses a key for co-signing the digital asset owner's transactions. • The digital asset owner and the DAC are required to cooperate as part of the signing process. • Signing process without the other, such as in emergency, depends on the service level agreement terms on key management model of the custody solution.
<p>Third-party custody</p>	<ul style="list-style-type: none"> • Funds are managed and held entirely by the DAC – the most robust level of third-party control. • The digital asset owner is not involved as a direct signing authority. • Service level agreements dictate the terms and timing conditions regarding the storage, access and movement of the digital assets by the DAC. • May be suitable for institutional investors such as asset managers, hedge funds or high-net-worth investors.

2.4 In the context of the regulatory framework for DACs in Malaysia, due to the Control Element as stipulated in Paragraph 1.2 of this Article, it is our view that Type 1 (self-custody) may not fulfil the requirements of the SC under the DA Guidelines. On the other hand, Type 2 (partial custody) and Type 3 (third-party custody) appear to be in compliance with the requirements under the DA Guidelines, provided that the relevant service level agreements shall permit the DAC to effect the transfer of the digital assets unilaterally under certain agreed circumstances, such as the demise of the digital asset owner.

- 2.5 Given the SC's emphasis on protection of investors' assets (for example, the requirements on ensuring that the digital asset owners have access to their digital assets at all times and preventing unauthorised access to the digital assets, ensuring that the employees that are involved in the key generation process are identified and prevented from having unauthorised access to clients' digital assets), we foresee that a role-based permissioning system, which has been adopted by certain DACs operating in other jurisdictions will be useful to outline the required system.
- 2.6 With role-based permissioning, coupled with strong governance and control protocols, certain key features may be observed:
- (a) Different components of the custody transaction are permissioned to separate personnel of the digital asset custody such that no single person can take over or corrupt the asset-moving process in isolation.
 - (b) Dual control should be required at as many steps in the asset movement workflow as possible, and it should require ideally three or four employees to effect digital asset movements. Company leaderships should have no ability to move assets or make system changes in isolation.
 - (c) There should be review processes to verify the legitimacy of client identity and instructions, preventing the tampering of data or manipulation of instructions.
 - (d) There should be internal activity logging that transcribes who does what and when, with broadcast mechanisms that notify key personnel of critical actions.
 - (e) System upgrades or changes shall require the operation of multiple personnel, preferably from different departments.

3. Perspective

- 3.1 DAC is a crucial component in ensuring the security, transparency and reliability of fundraising via an IEO. In addition to regulating the IEO operator, the entrustment of the storing and custody of digital tokens to a DAC, who in turn is also subject to a separate set of standards of conduct, duties and obligations as set out in Part D of the DA Guidelines, serves to further protect the interest of the investors in an IEO.
- 3.2 In contrast to an IEO operator which must be a Malaysian-incorporated company, a DAC can be either a local or foreign entity subject to satisfaction of the requirements under Part D of the DA Guidelines, although a foreign applicant is required to fulfil certain additional criteria, including demonstrations that it is in the best interest of Malaysia to register the foreign DAC and it is authorised to operate or carry out an activity of a similar nature in the foreign jurisdiction. Despite the higher threshold for foreign DAC applicants, it is arguably a good opportunity for foreign digital asset custody service providers to enter this relatively new and emerging market in Malaysia. Given that there are currently no existing registered DACs in Malaysia, foreign DAC applicants who have operated such a business within the regulatory framework of their respective jurisdiction may have a competitive edge by virtue of their existing resources and expertise.
- 3.3 It is also apparent under the DA Guidelines that the SC has considerable powers in respect of a DAC, including powers to issue directions to the DAC, its directors or senior

management and to periodically assess the DAC's compliance with any or all of its regulatory obligations. The powers of the SC even extend to parties who have been outsourced with certain functions by the DAC. In relation thereto, where an outsourcing arrangement is categorised as material pursuant to the DA Guidelines, the DAC is required to, among others, obtain a written undertaking from the outsourced party to provide the SC with access to all information concerning such material outsourced arrangement. As such, while a DAC has the autonomy to provide custody services for the investors' digital assets on its own terms, the DA Guidelines provides adequate checks and balances to monitor the DAC's conduct.

- 3.4 The application to become a registered DAC is currently open and we understand that no deadline has been imposed by the SC on such registration process at this juncture.

In the previous chapters of our Digital Assets Series, we offer a brief introduction to digital assets and its regulatory framework in Malaysia ([Chapter 1](#)), and addressed IEO and the regulatory framework for IEO operators in Malaysia ([Chapter 2](#)).

In the next chapter of our Digital Assets Series (Chapter 4), we will consider the regulatory framework for issuers seeking to raise funds via IEO in Malaysia.

This legal update is for general information only and is not a substitute for legal advice.

Further Information

Should you have any queries as to how these developments may affect your business, please do not hesitate to contact us.



Yau Khai Ling
Principal
E: ykl@khailinglaw.com



Lau Yuet Sian
Senior Legal Associate
E: lys@khailinglaw.com



Lee Zi Hong
Legal Associate
E: lzh@khailinglaw.com



Rachel Lim Ze Xing
Junior Legal Project Manager
E: corporate@khailinglaw.com

For more information on other insights shared by KhaiLing Yau Chambers, please click [here](#).