

The Revised Guidelines on Digital Assets

03 DECEMBER 2020

On 28 October 2020, the Securities Commission Malaysia ('SC') issued the revised [Guidelines on Digital Assets](#) ('Guidelines') which came into effect immediately.

The Guidelines superseded a draft that was released by the SC on 15 January 2020 ('Draft Guidelines') for the purpose of enabling potential issuers, platform operators and investors to familiarise themselves with the framework and requirements for the offering of digital tokens under an initial exchange offering ('IEO') and for operating an electronic platform for hosting IEOs of digital tokens ('IEO platform').

The SC also announced in its [media release](#) of 28 October 2020 that parties who are interested to be registered as an operator of an IEO platform ('IEO operator') or as a custodian for digital assets may submit their applications to the SC on or before **15 February 2021**.

The SC has also reminded the public in its media release that no person is permitted to offer, issue or distribute any digital assets in Malaysia without obtaining a registration or authorisation under the Guidelines.

This note highlights some of the main requirements set out the Guidelines.

A. OVERVIEW

The Guidelines are divided into five (5) parts. **Part A** sets out the general provisions, **Part B**, the requirements relating to digital token offerings, **Part C**, the requirements relating to an IEO operator, **Part D**, the requirements relating to a digital asset custodian and **Part E**, the submission of applications.

The main differences from the Draft Guidelines are as follows:

1. A new Part D has been introduced to set out the requirements in relation to a digital asset custodian;
2. The Guidelines now permit a limited liability partnership ('LLP') registered under section 11 of the Limited Liability Partnerships Act 2012 ('LLP Act') to raise funds through a digital token offering; and
3. The responsibilities of the directors of an IEO operator have been set out in greater detail; some of these responsibilities are new whereas others had been imposed on the IEO operator under the Draft Guidelines.

B. DIGITAL TOKEN OFFERINGS

1. *The issuer*

An issuer ('issuer') must satisfy the following criteria in order to raise funds through an IEO of digital tokens under the Guidelines:

1.1 *The issuer*

The issuer must be:

- (a) a company incorporated in Malaysia, but must not be an exempt private company or a public listed company; an unlisted subsidiary or a special purpose vehicle of a public listed company may be an issuer; or
- (b) a LLP registered under section 11 of the LLP Act; it appears that a conventional partnership or a limited liability company that converted to a LLP and was registered pursuant to section 32 of the LLP Act and a foreign LLP registered under section 45 of the LLP Act are ineligible to raise funds through an IEO under the Guidelines.

1.2 Place of operations

The issuer must have its main business operations in Malaysia.

1.3 Source of fund raising

An issuer must only raise funds through an IEO through an IEO platform and not through other means.

1.4 Financial requirements

- (a) An issuer must have a minimum paid-up capital of RM500,000 and at all times maintain a minimum shareholders' funds of RM500,000. Where an issuer is a LLP, it must at all times maintain a minimum capital of RM500,000.
- (b) The SC may at any time impose additional financial requirements that commensurate with the nature, operations and risks posed by the issuer.

1.5 Directors and senior management

- (a) An issuer must, at all times, have at least two directors whose principal or only place of residence is in Malaysia.
- (b) An issuer must ensure that its directors and senior management are fit and proper in accordance with the criteria in Appendix 1 of the Guidelines.

1.6 Moratorium on equity interest

- (a) The directors and senior management of an issuer must, in the aggregate, own at least 50% equity holding in the issuer on the date of issuance of the digital tokens.
- (b) Subsequent to the issuance of the digital tokens, the issuer's directors and senior management (including those who are subsequently appointed as directors or senior management who purchase their equity in the issuer after issuance of the digital tokens) may only sell, transfer or assign not more than 50% of their respective equity holding until the completion of the IEO project.

2. Application to raise funds through IEO

2.1 Approval requirement

- (a) An issuer must submit its application ('application') to raise funds through an IEO to an IEO operator for approval in the form and manner specified by the IEO operator.
- (b) An issuer must ensure that the application includes:

- (i) a fit and proper declaration of all the issuer's directors and senior management; and
- (ii) the white paper ('white paper') which must contain the information specified in paragraphs 8.03 and 8.04 of the Guidelines.

2.2 Offering of digital tokens

An issuer must not offer any digital tokens to any person before the IEO operator's approval for the application has been obtained.

2.3 Innovative solution or meaningful digital proposition

In its application, the issuer must demonstrate to the IEO operator that the IEO project provides an innovative solution or a meaningful digital value proposition for Malaysia. By way of guidance, the Guidelines clarify that an IEO project provides an innovative solution or digital value proposition if, among others, the IEO project:

- (a) provides a solution to, or addresses, an existing market need or problem; or
- (b) improves the efficiency of an existing process or service undertaken by the issuer or the industry.

2.4 Closed loop

If a digital token serves as a payment instrument, it may only be used in exchange for an issuer's goods and services as disclosed in the issuer's white paper approved by the IEO operator.

3. Limit on fundraising

- (a) An IEO operator must ensure that the amount raised by an issuer within any continuous 12-month period must not exceed 20 times of the amount of an issuer's shareholders' funds (or in the case of an LLP, the issuer's capital), subject always to a ceiling of RM100 million.
- (b) The issuer must demonstrate to the IEO operator that the gross proceeds to be raised from the IEO will be sufficient to undertake the IEO project as proposed in the white paper.
- (c) The digital tokens to be issued by an issuer must be fully subscribed; an issuer is not allowed to keep any amount exceeding the target amount raised.
- (d) In the case of under-subscription, the IEO operator must return all monies collected from the token holders within six (6) business days of the closing of the offer period.

4. Investment limits

The following limits apply to investments in a digital token offering:

- (a) For sophisticated investors: no restriction;
- (b) For angel investors: a maximum of RM500,000 within a 12-month period;
- (c) For retail investors: a maximum of RM2,000 per issuer with a total investment limit not exceeding RM20,000 within a 12-month period.

5. *Cooling-off right*

- (a) An applicant who subscribes for a digital token in an IEO must be given a cooling-off right, except where the applicant is a staff of the issuer.
- (b) The cooling-off period must not be less than six (6) business days commencing from the closing date of the offer period.
- (c) When an applicant exercises the cooling-off right, he shall be entitled to a refund of a sum equal to the aggregate of the purchase price paid for the digital token and any other charges imposed on the day the digital token was purchased.
- (d) The refund is to be made by the IEO operator within six (6) business days from its receipt of the notification of exercise of the cooling-off right by the investor.

6. *The white paper*

6.1 *Submission of white paper*

- (a) An issuer is not permitted to offer a digital token to any person unless the offer is accompanied by a white paper that has been approved by the IEO operator.
- (b) An issuer must furnish to the SC a copy of the white paper that has been furnished to the IEO operator.

6.2 *Contents of the white paper*

- (a) An issuer must ensure that the white paper contains such information that would enable an investor to make an informed assessment of the digital token before subscribing for the digital token. Such information would include the following:
 - (i) a brief description of the issuer's directors, senior management, key personnel and advisers, including their names, designations, nationalities, addresses, professional qualifications and related experience;
 - (ii) the objective or purpose of the IEO, including detailed information on the IEO project to be managed and operated by the issuer;
 - (iii) the key characteristics of the digital token;
 - (iv) a detailed description of the sustainability and scalability of the IEO project;
 - (v) the business plan of the issuer;
 - (vi) the targeted amount to be raised through the IEO, and the subsequent use and application of the proceeds, illustrated in a scheduled timeline for drawdown and utilisation of the proceeds;
 - (vii) any rights, conditions or functions attached to the digital tokens including any specific rights attributed to a token holder;
 - (viii) a discussion on the determination of the accounting and the valuation treatments for the digital token including all valuation methodologies and reasonable presumptions adopted in such calculation;
 - (ix) associated challenges and risks as well as the mitigating measures thereof;

- (x) the information relating to the distribution of the digital tokens, and where applicable, the distribution policy of the issuer;
 - (xi) a technical description of the protocol, platform or application of the digital token, as the case may be, and the associated benefits of the technology; and
 - (xii) the audited financial statements of the issuer.
- (b) A white paper must also include the following statements:
- (i) that the furnishing of the white paper to the SC should not be taken as an indication that the SC assumes responsibility for the correctness of any statement made in the white paper; and
 - (ii) that Bank Negara Malaysia does not recognise digital tokens as legal tender or as a payment instrument regulated by it and that it will not provide any avenue of redress for aggrieved token holders.

7. Obligations of an issuer

7.1 General

An issuer must, amongst its obligations:

- (a) comply with the requirements of the Guidelines at all times;
- (b) ensure that it does not submit or provide any document or information that is false or misleading, or from which there is material omission;
- (c) submit to the IEO operator a fit and proper declaration of its directors and senior management within three (3) business days from the appointment or reappointment of the director or senior management;
- (d) immediately notify the IEO operator and the SC of any failure to comply with any requirement of the Guidelines;
- (e) retain all relevant documents related to the IEO for seven (7) years from the date the documents or agreements are submitted to the IEO operator; and
- (f) provide to the SC any information or assistance relating to the digital tokens as the SC deems necessary.

7.2 Utilisation of proceeds

- (a) An issuer must provide a confirmation to the SC that the drawdowns have been utilised for the purposes stated in the white paper;
- (b) An issuer must not make any changes to the utilisation of proceeds after the issuance of the digital tokens or any changes that affect the token holders' rights, unless the prior approval of the token holders representing 75% of the total amount of tokens held by all token holders present and voting has been obtained.

7.3 Managing conflicts

An issuer must establish a framework which sets out the policies and procedures to effectively and efficiently manage issues of conflict of interest, actual or potential, and any related party transaction which may arise in the course of the IEO project.

8. *Hosting on multiple platforms*

An issuer must not be hosted concurrently on multiple IEO platforms or on an equity crowdfunding or peer-to-peer (P2P) platform.

9. *Material changes*

- (a) An issuer must inform the IEO operator of any material change that affects the IEO, the IEO project or the issuer immediately upon knowing or becoming aware of the change for the purposes of announcement on the IEO platform.
- (b) Post issuance of the digital tokens, the issuer must also immediately notify the IEO operator of any sale, transfer or assignment involving 5% or more shareholding in the issuer.

10. *Reporting and audit*

- (a) An issuer must prepare and cause to be published on the IEO platform an annual report and semi-annual report which contain necessary information that enables token holders to evaluate the performance of the issuer.
- (b) The issuer's report must contain information on the performance of the underlying business or project, including:
 - (i) the total amount of digital tokens issued and in circulation;
 - (ii) the status of the utilisation of the digital token's proceeds by the issuer;
 - (iii) the status of the IEO project; and
 - (iv) the audited financial statements of the issuer for its latest financial year.

11. *Marketing and promotion*

- (a) An issuer must ensure that all information disseminated for marketing or promotion is consistent with the contents of the white paper.
- (b) An issuer must not engage any third party individual or entity, other than an IEO operator, to endorse or represent the issuer with the intended purpose of marketing, promoting, gaining publicity or soliciting funds for its IEO.

C. THE IEO OPERATOR

1.1 *Application and registration requirements*

- (a) A person who seeks to operate an IEO platform must be registered under the Guidelines.
- (b) Where a person who seeks to operate an IEO platform also seeks to facilitate the trading of digital assets on its platform, it must also be registered as a digital assets exchange (DAX) operator under the Guidelines on Recognised Markets.

1.2 *Registration*

- (a) The SC may register a person as an IEO operator, subject to the person satisfying the requirements in Part C of the Guidelines.

- (b) The application to the SC must be made by the operator of the IEO platform.
- (c) An IEO operator registered under the Guidelines is deemed to be registered as a recognised market operator for the purposes of section 34 of the Capital Markets and Services Act 2007.

1.3 Application

An applicant is required to submit to the SC the relevant forms and documents specified in Appendix 2 of the Guidelines and any other information required by the SC. The application is to be accompanied by the prescribed fees.

1.4 Incorporation

An IEO operator must be a Malaysian-incorporated company unless specified otherwise by the SC.

1.5 Financial requirements

- (a) An IEO operator must have a minimum paid-up capital of RM5,000,000.
- (b) The SC may at any time impose additional financial requirements on an IEO operator that commensurate with the nature, operation and risks posed by the IEO operator.
- (c) An IEO operator must immediately notify the SC in writing of a potential or an actual breach of the minimum financial requirement and the corrective measures intended to be taken to address the potential or actual breach.

2. Criteria for registration

The SC may register an applicant as an IEO operator if it is satisfied that all of the following requirements have been fulfilled:

- (a) the applicant, its directors, controller and senior management are fit and proper in accordance with the criteria in Appendix 1 of the Guidelines;
- (b) the applicant will be able to carry out its obligations under the Guidelines;
- (c) the applicant will appoint at least one (1) responsible person as required under Chapter 16 of the Guidelines;
- (d) the applicant will be able to manage risks associated with its business and operations, including demonstrating the processes and contingency arrangement in the event that it is unable to carry out its operations;
- (e) the applicant has sufficient financial, human and other resources for its operations at all times; and
- (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 SC's Guidelines on Management of Cyber Risk and other relevant guidelines.

3. Directors, senior management and responsible person

3.1 Independent Director

An IEO operator which is a public company must have at least one (1) independent director.

3.2 Directors and senior management

- (a) An IEO operator must ensure that its directors, controller and senior management are fit and proper in accordance with the criteria in Appendix 1 of the Guidelines and are suitably qualified.
- (b) An IEO operator must notify the SC in writing of any appointment or reappointment of a director, within such time as specified by the SC or prior to any public announcement on such appointment or reappointment, whichever is the earlier.
- (c) Where a director or senior management is no longer fit and proper to hold office, the IEO operator must ensure that the person concerned vacates his office immediately.
- (d) The IEO operator must immediately notify the SC of a director's or senior management's disqualification and when the position is vacated.

3.3 Responsible Person

- (a) An IEO operator must have at least one (1) responsible person at all times.
- (b) The responsible person must be appointed from the IEO operator's senior management.
- (c) The responsible person must at all times undertake the role of the main contact person to liaise with the SC and perform any duty as may be directed by the SC.
- (d) The responsible person must have a minimum of five (5) years' experience in carrying out due diligence, assessment on business proposals and fundraising or any other relevant experience, and must be a fit and proper person in accordance with the criteria in Appendix 1 of the Guidelines.
- (e) Any vacancy in the position of a responsible person is to be filled within one (1) month from the date the vacancy arises.

4. Obligations of the parties

4.1 Senior management's obligations

The senior management must, among others:

- (a) implement and adhere to the policies, practices and standards approved by the board of the IEO operator;
- (b) manage risks associated with the business of an IEO operator including performing periodic evaluation of its risk management process;
- (c) frequently and adequately appraise the board of the IEO operator on the operations of the IEO operator; and

- (d) ensure that all records of transactions relating to investors and all records that sufficiently explain the financial position and the business of the IEO operator are accurate, properly secured, and retained for a minimum period of seven (7) years.

4.2 **Obligations of the board**

The board of an IEO operator must, among others:

- (a) ensure the IEO operator complies with the requirements of securities laws and the Guidelines and any direction issued or term or condition imposed by the SC;
- (b) ensure the responsible person carries out his responsibilities and duties;
- (c) identify and manage risks associated with the business and operations of the IEO operator, including having in place an effective business continuity plan;
- (d) establish and maintain policies and procedures to:
 - (i) effectively and efficiently manage actual and potential conflicts of interest;
 - (ii) implement anti-corruption and whistleblowing measures that are appropriate to the nature, scale and complexity of the IEO operator's business; and
 - (iii) monitor the offering and other market activity to detect non-compliance with the securities laws or the IEO operator's rules;
- (e) define and oversee the business plan and strategy of the IEO operator that is appropriate to its objective, size, structure and risk profile;
- (f) ensure that the IEO operator has the relevant capabilities including technology capabilities and support, secured infrastructure and sufficient resources to undertake its business;
- (g) approve and oversee all key policies including those relating to risk management, internal controls and compliance with the requirements under securities laws and guidelines or industry best practices;
- (h) ensure all policies, processes and procedures are continuously reviewed so that they remain relevant and effective, taking into consideration developments in the IEO operator's business and operations; and
- (i) immediately notify the SC:
 - (i) of any irregularity or breach of any provision of the securities laws, the Guidelines or the IEO operator's rules, including any alleged or suspected violations of any law or guidelines in relation to money laundering, terrorism financing and proliferation financing by its participants;
 - (ii) of any material change in the information submitted to the SC; or
 - (iii) if it becomes aware of any matter which adversely affects or is likely to adversely affect the ability of the IEO operator to meet its obligations.

4.3 Obligations of the IEO operator

4.3.1 Evaluating an IEO

In determining whether to approve an IEO, an IEO operator must:

- (a) carry out due diligence and critical assessment on an issuer, including:
 - (i) understanding and verifying the business of the issuer to ensure that the issuer does not engage in any business practices that appear to be deceitful, oppressive or improper, whether unlawful or not;
 - (ii) assessing the fit and properness of the issuer's directors and senior management; and
 - (iii) understanding the features of the digital token to be issued by the issuer and the rights attached to it;
- (b) exercise its own judgment and carry out critical assessment on the issuer's compliance with the requirements of the Guidelines, including whether the issuer will be able to satisfy the requirement to provide an innovative solution or meaningful digital value proposition for Malaysia; and
- (c) assess the issuer's white paper; in approving the issuer's white paper, the IEO operator must ensure that the contents of the white paper include the information specified in the Guidelines and are not false or misleading, or contain any material omission;

4.3.2 Other obligations of an IEO operator

An IEO operator must also comply with the requirements set out in paragraph 17.04 of the Guidelines. These requirements include:

- (a) ensuring that the issuer's white paper is accessible to investors through its IEO platform;
- (b) ensuring that all relevant information relating to an issuer, including any material changes that affect the IEO project or the issuer and the issuer's annual and semi-annual report are available through its IEO platform;
- (c) taking reasonable steps to monitor the drawdowns by the issuer and that they have been utilised for the purposes stated in the white paper;
- (d) ensuring that its IEO platform is operating in an orderly, fair and transparent manner;
- (e) having in place rules and procedures for the IEO on its IEO platform;
- (f) taking all reasonable measures to avoid situations that are likely to involve a conflict of interest with the issuer;
- (g) disclosing any information and providing any document to the SC as it may require;
- (h) ensuring that all disclosures are not false or misleading or contain any material omission;

- (i) obtaining and retaining self-declared risk acknowledgment forms from its users prior to them investing in the IEO;
- (j) providing prior disclosure to investors that any loss resulting from investing in an IEO is not covered by the Capital Market Compensation Fund;
- (k) disclosing and displaying prominently on its IEO platform any relevant information relating to the recognised market, including:
 - (i) all necessary risk warning statements, including all risk factors that users may require in making a decision to participate on the IEO platform;
 - (ii) information on rights of investors to investing in a recognised market;
 - (iii) criteria for access to the recognised market;
 - (iv) fees, charges and other expenses that it may charge or impose on its users;
 - (v) information on processes and contingency arrangement in the event that it is unable to carry out its operations or cessation of business; and
 - (vi) any other information as may be specified by the SC;
- (l) establishing and maintaining policies and procedures to:
 - (i) provide clear line of reporting, authorisation and proper segregation of functions;
 - (ii) implement anti-corruption and whistleblowing measures that are appropriate to the nature, scale and complexity of its business;
 - (iii) identify, monitor, manage and mitigate cyber risks in its operating environment;
 - (iv) effectively and efficiently identify, monitor, mitigate and manage situations and potential situations which may give rise to conflicts of interest; and
 - (v) ensuring compliance with all relevant laws and guidelines, including anti-money laundering and anti-terrorism financing laws and personal data protection laws;
- (m) ensuring that its processes and practices are continuously aligned to industry practices in relation to digital assets;
- (n) taking all reasonable steps to ensure fair treatment of clients;
- (o) identifying and managing potential vulnerabilities and cyber threats in its operating environment;
- (p) in the event of any systems error, failure or malfunction, taking all necessary and immediate appropriate actions to mitigate any potential losses;

- (q) carrying out any other duties or responsibilities as may be specified by the SC;
- (r) immediately notifying the SC:
 - (i) of any breach of the terms and conditions imposed by the SC, or any provisions of the securities laws, guidelines or the IEO operator's rules, including any alleged or suspected violations of the aforesaid laws or guidelines (including anti-money laundering and anti-terrorism financing laws and personal data protection laws);
 - (ii) when it becomes aware of any matter which adversely affects or is likely to adversely affect its ability to meet its obligations or to carry out its functions under the Guidelines;
 - (iii) of any material adverse change to the IEO, the IEO project or the issuer including:
 - the discovery of any false or misleading statement in any disclosures in relation to the IEO, the IEO project or the issuer;
 - the discovery of any material omission of information that may affect token holders; or
 - any material development in the circumstances relating to the IEO, the IEO project or the issuer; and
 - (iv) of the occurrence of any event which would trigger the activation or execution of the business continuity plan;
- (s) retaining for a minimum period of seven (7) years all records relating to its investors and all records that sufficiently explain its financial position and the business; and
- (t) providing the SC with access to any register required to be maintained under the Guidelines and disclosing any other information as the SC may require.

4.3.3 Rules of the IEO operator

Any proposed rules of an IEO operator and any proposed amendments to the existing rules of an IEO operator shall not have effect unless they have been approved by the SC.

4.3.4 Risk management

An IEO operator must comply with the risk management requirements set out in paragraphs 17.06 to 17.10 of the Guidelines, which include identifying and mitigating possible operational risks, having a business continuity plan and carrying out periodic reviews, audits and testing on its systems, operational policies, procedures and controls relating to risk management and its business continuity plan.

4.3.5 Internal audit

An IEO operator must establish an internal audit function to develop, implement and maintain an appropriate internal audit framework which commensurate with its business and operations.

4.3.6 Managing conflicts of interest

In relation to managing conflicts of interest:

- (a) an IEO operator, including all its directors and shareholders, must disclose to the public on its platform if:
 - (i) it holds any shares in any of the issuers or digital tokens issued by any issuers hosted on its platform; or
 - (ii) it pays any referrer or introducer, or receives payment in whatever form, in connection with an issuer hosted on its platform;
- (b) an IEO operator must ensure that its shareholding in any issuer hosted on its platform must not exceed 30%; and
- (c) an IEO operator is prohibited from providing direct or indirect financial assistance to investors to invest in the digital tokens of an issuer hosted on its platform.

4.3.7 Operation of trust account

An IEO operator must, among others:

- (a) establish systems and controls for maintaining accurate and up-to-date records of investors and any monies or digital tokens held in relation to the investor;
- (b) ensure investors' monies and digital tokens are properly safeguarded from conversion or inappropriate use by any person, including but not limited to implementing multi-signature arrangements;
- (c) establish and maintain with a licensed Malaysian financial institution one or more trust accounts, designated for monies received from investors;
- (d) ensure that the trust accounts are administered by an independent trustee registered with the SC under the Guidelines on Registration and Conduct of Capital Market Services Providers;
- (e) only release the funds to the issuer after the targeted amount sought to be raised has been met and there is no material change relating to the IEO or the issuer during the offer period; an IEO operator may impose any other additional condition precedent before releasing the funds, provided that they serve the token holders' interest; and
- (f) ensure that the token holders' digital tokens are properly segregated and establish and maintain a sufficiently and verifiably secured storage medium designated to store digital assets from investors. In this regard, an IEO operator may:
 - (i) appoint a digital asset custodian registered with the SC under Part D of the Guidelines to provide custody of the token holders' digital tokens; or
 - (ii) provide its own custody services to the token holders provided that the IEO operator ensures that it complies with the requirements set out in Part D of the Guidelines.

4.3.8 Register of initial token holders

An IEO operator must maintain a register of initial token holders who subscribed for the digital tokens during the offer period and enter into the register the information prescribed in paragraphs 17.20(a) to 17.20(d) of the Guidelines.

4.3.9 Outsourcing of functions

- (a) Save and except for any function that involves the decision making functions of the IEO operator or any interaction or direct contact with the IEO issuer or token holders, an IEO operator may outsource its functions to service providers, subject to compliance with the requirements set out in paragraphs 17.21 to 17.31 of the Guidelines. The board of directors of the IEO operator remains accountable for all outsourced functions.
- (b) An IEO operator is also required to provide the SC with information on outsourcing arrangements in the circumstances set out in paragraphs 17.32 and 17.33 of the Guidelines.

5. Other requirements

Chapter 28 of the Guidelines imposes obligations on an IEO operator in relation to restrictions and limits on funds raised by an issuer on an IEO operator's platform, investment limits imposed on investors and the cooling off rights of investors. These are dealt with in paragraphs 3 to 5 of Part B of this write-up.

6. Cessation of business operations

- (a) An IEO operator shall not cease its business or operations without prior engagement with the SC.
- (b) The SC may issue a direction or impose any term or condition for the purposes of ensuring the orderly cessation of the business or operations of an IEO operator.
- (c) The cessation of business or operations of an IEO operator will not take effect until the SC is satisfied that all requirements stated in the securities laws, the Guidelines, relevant guidelines issued by the SC and any other relevant laws or requirements, have been fulfilled.

D. DIGITAL ASSET CUSTODIAN

1.1 Introduction

- (a) The services of providing safekeeping, storing, holding or maintaining custody of digital assets for the account of another person is specified to be a capital market services for the purposes of section 76A of the Capital Markets and Services Act 2007.
- (b) For the purposes of Part D of the Guidelines, a digital asset custodian refers to a person who provides any of the services described in sub-paragraph (a) above.
- (c) A registered recognised market operator or registered trustee who seeks to provide any of the services specified in sub-paragraph (a) above must notify the SC of its intention prior to providing the specified services. The SC may carry out an assessment on the registered recognised market operator or registered trustee who shall be deemed to be registered as a digital asset custodian under the Guidelines provided that the SC is

satisfied that such operator or trustee is able to comply with the requirements set out in Part D of the Guidelines.

1.2 Registration

- (a) The SC may register a person as a digital asset custodian if it satisfies the requirements set out in Part D of the Guidelines.
- (b) The SC may register a **foreign** digital asset custodian as a digital asset custodian if, in addition to satisfying the requirements in Part D of the Guidelines, the SC is satisfied that:
 - (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 digital asset custodian, taking into consideration any one or more of the factors set out in paragraph 23.06 of the Guidelines.

1.3 The application

An applicant is required to submit to the SC the relevant forms and documents specified in Appendix 3 of the Guidelines and any other information required by the SC. The application is to be accompanied by the prescribed fees.

2. Financial requirements

- (a) A digital asset custodian must have a minimum paid-up capital of RM500,000 and maintain a minimum shareholders' fund of RM500,000 at all times.
- (b) The SC may at any time impose additional financial requirements on a digital asset custodian that commensurate with the nature, operation and risks posed by the digital asset custodian.
- (c) A digital asset custodian must immediately notify the SC in writing of a potential or an actual breach of the minimum financial requirements and the corrective measures intended to be taken to address the potential or actual breach.

3. Criteria for registration

The SC may register an applicant as a digital asset custodian if it is satisfied that all of the following requirements have been fulfilled:

- (a) the applicant, its directors, controller and senior management are fit and proper in accordance with the criteria in Appendix 1 of the Guidelines;
- (b) the applicant will be able to carry out its obligations under the Guidelines;
- (c) the applicant will appoint at least one (1) responsible person as required under Chapter 26 of the Guidelines;
- (d) the applicant will be able to manage risks associated with its business and operations, including demonstrating the processes and contingency arrangement in the event that it is unable to carry out its operations;

- (e) the applicant has sufficient financial, human and other resources for its operations at all times; and
- (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 SC's Guidelines on Management of Cyber Risk and other relevant guidelines.

4. Directors, senior management and responsible person

4.1 Directors and senior management

- (a) A digital asset custodian must ensure that its directors, controller and senior management are fit and proper in accordance with the criteria in Appendix 1 of the Guidelines and are suitably qualified.
- (b) Where a director or senior management is no longer fit and proper to hold office, the digital asset custodian must ensure that the person concerned vacates his office immediately.
- (c) The digital asset custodian must immediately notify the SC of a director's or senior management's vacation from office.

4.2 Responsible Person

- (a) A digital asset custodian must have at least one (1) responsible person at all times.
- (b) The responsible person must be appointed from the digital asset custodian's senior management.
- (c) The responsible person must at all times undertake the role of the main contact person to liaise with the SC and perform any duty as may be directed by the SC.
- (d) The responsible person must have a minimum of five (5) years of relevant industry experience or expertise and must be a fit and proper person in accordance with the criteria in Appendix 1 of the Guidelines.
- (e) Any vacancy in the position of a responsible person is to be filled within one (1) month from the date the vacancy arises.

5. Obligations of the parties

5.1 Senior management's obligations

The senior management must, among others:

- (a) implement and adhere to the policies, practices and standards approved by the board of the digital asset custodian;
- (b) manage risks associated with the business of a digital asset custodian including performing periodic evaluation of its risk management process;
- (c) frequently and adequately appraise the board of the digital asset custodian on the operations of the digital asset custodian; and
- (d) ensure that all records of transactions relating to clients and all records that sufficiently explain the financial position and the business of the digital asset

custodian are accurate, properly secured, and retained for a minimum period of seven (7) years.

5.2 **Obligations of the board and chief executive**

The board and chief executive of a digital asset custodian must, among others:

- (a) ensure the digital asset custodian complies with the requirements of securities laws and the Guidelines and any direction issued or term or condition imposed by the SC;
- (b) ensure the responsible person carries out his responsibilities and duties;
- (c) identify and manage risks associated with the business and operations of the digital asset custodian, including having in place an effective business continuity plan;
- (d) establish and maintain policies and procedures to:
 - (i) effectively and efficiently manage actual and potential conflicts of interest;
 - (ii) implement anti-corruption and whistleblowing measures that are appropriate to the nature, scale and complexity of the digital asset custodian's business; and
 - (iii) monitor the transfer of digital assets to detect non-compliance with the securities laws or the digital asset custodian's rules;
- (e) define and oversee the business plan and strategy of the digital asset custodian that is appropriate to its objective, size, structure and risk profile;
- (f) ensure that the digital asset custodian has the relevant capabilities including technology capabilities and support, secured infrastructure and sufficient resources to undertake its business;
- (g) approve and oversee all key policies including those relating to risk management, internal controls and compliance with the requirements as provided under the securities laws, relevant laws and guidelines or industry best practices;
- (h) ensure all policies, processes and procedures are continuously reviewed so that they remain relevant and effective, taking into consideration developments in the digital asset custodian's business and operations;
- (i) ensure that the clients' digital assets are safeguarded; and
- (j) immediately notify the SC:
 - (i) of any irregularity or breach of any provision of the securities laws, the Guidelines or the digital asset custodian's rules, including any alleged or suspected violations of any law or guidelines relating to money laundering, terrorism financing and proliferation financing by its participants;
 - (ii) of any material change in the information submitted to the SC; or
 - (iii) if it becomes aware of any matter which adversely affects or is likely to adversely affect the ability of the digital asset custodian to meet its obligations.

5.3 Obligations of a digital asset custodian

A digital asset custodian must comply with the requirements set out in paragraph 27.03 of the Guidelines. These requirements include:

- (a) acting in the best interest of the clients and taking all reasonable measures to avoid situations that are likely to involve conflict of interest with the clients;
- (b) safeguarding the rights and interest of its clients including ensuring that its clients have access to their digital assets at all times, and preventing unauthorised access to the clients' digital assets;
- (c) disclosing any information and providing any document to the SC as it may require;
- (d) complying with all reporting requirements and submitting accurate information required by the SC in a timely manner;
- (e) identifying and managing risks associated with the business and operations of the digital asset custodian, including having in place an effective business continuity plan;
- (f) establishing and maintaining written policies and procedures to:
 - (i) provide clear line of reporting, authorisation and proper segregation of functions;
 - (ii) prevent unauthorised access or fraudulent transaction;
 - (iii) implement anti-corruption and whistleblowing measures that are appropriate to the nature, scale and complexity of its business;
 - (iv) enable full disclosure of all client's transactions and assets to the client;
 - (v) ensuring compliance with all relevant laws and guidelines, including anti-money laundering and anti-terrorism financing laws and personal data protection laws;
 - (vi) managing clients' data that cover collection, storage, use, disclosure and disposal of client information, including the following:
 - proper handling and safeguarding of client data;
 - protection of confidentiality and security of client data; and
 - managing third party service provider who has access to client data;
- (g) ensuring that its processes and practices are continuously aligned to industry practices in relation to the custody of digital assets;
- (h) taking all reasonable steps to ensure fair treatment of clients;
- (i) identifying and managing potential vulnerabilities and cyber threats in its operating environment;
- (j) in the event of any systems error, failure or malfunction, taking all necessary and immediate appropriate actions to mitigate any potential losses;

- (k) carrying out any other duties or responsibilities as may be specified by the SC;
- (l) immediately notifying the SC:
 - (i) of any breach of the terms and conditions imposed by the SC, or any provisions of the securities laws, guidelines or the digital asset custodian's rules, including any alleged or suspected violations of any relevant laws or guidelines relating to anti-money laundering and anti-terrorism financing and personal data protection;
 - (ii) when it becomes aware of any matter which adversely affects or is likely to adversely affect its ability to meet its obligations or to carry out its functions under the Guidelines; and
 - (iii) of the occurrence of any event which would trigger the activation or execution of the business continuity plan;
- (m) retaining for a minimum period of seven (7) years all records relating to its clients and all records that sufficiently explain the financial position and the business of the digital asset custodian; and
- (n) providing the SC with access to any register required to be maintained under the Guidelines and disclosing any other information as the SC may require.

5.4 Risk management

A digital asset custodian must comply with the risk management requirements set out in paragraphs 27.04 to 27.06 of the Guidelines, which include identifying, assessing, monitoring, controlling and reporting all material risks to which it could be exposed, and carrying out periodic reviews, audits and testing on systems, operational policies, procedures and controls relating to risk management and its business continuity plan.

5.5 Managing conflicts of interest

- (a) A digital asset custodian must give priority to the clients' interest if there is a conflict between the clients' interest and its own interest.
- (b) A digital asset custodian must establish and maintain written policies and processes and procedures that:
 - (i) identify, monitor, mitigate and manage situations and potential situations which may give rise to conflicts of interest; and
 - (ii) require disclosure of any conflict or potential conflict of interest.

5.6 Internal audit

- (a) A digital asset custodian must perform internal audit checks on its operations regularly. For this purpose, a digital asset custodian may establish an internal audit function or outsource the said function.
- (b) The person responsible for the internal audit function must report directly to the board of the digital asset custodian on the adequacy, effectiveness and efficiency of the management, operations, risk management and internal controls.
- (c) The board of a digital asset custodian must ensure that the internal audit framework includes:

- (i) clearly defined terms which set out the scope, objectives, approach and reporting requirements;
 - (ii) adequate planning, controlling and recording all audit work performed, and record the findings, conclusions and if any, recommendations made;
 - (iii) issuance of an internal audit report at the conclusion of each internal audit performed; and
 - (iv) ensuring matters that are highlighted in the internal audit report are satisfactorily resolved in a timely manner and do not jeopardise or prejudice the clients' interest.
- (d) The internal audit framework must be approved by the board of the digital asset custodian.

6. Conduct requirements of a digital asset custodian

6.1 Key generation and management

- (a) A digital asset custodian must establish and maintain a sufficiently and verifiably secured storage medium designated to store its clients' digital assets.
- (b) A digital asset custodian must have in place effective policies and procedures to safeguard key generation and management including:
 - (i) adopting industry standards and practices in terms of key generation and management;
 - (ii) ensuring that the employees 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) A digital asset custodian must 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.

6.2 Segregation of client assets

A digital asset custodian must:

- (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 systems and controls for maintaining accurate and up-to-date records of clients' digital assets held.

6.3 Transaction handling

- (a) A digital asset custodian must ensure that, at all times, it has up-to-date transactional records relating to the clients' digital assets including:
 - (i) transaction timestamp;

- (ii) details of any transaction including the purpose of a transfer, amount and details of the counterparty;
 - (iii) relevant signatories and transaction approval/rejection evidence;
 - (iv) account balances;
 - (v) transaction value; and
 - (vi) any other information as may be specified by the SC.
- (b) The digital asset custodian must provide the information referred to in paragraph (a) above to the SC as and when requested by the SC.
- (c) The digital asset custodian must retain all the transactional records including those stated in paragraph (a) above for a minimum period of seven (7) years.

7. Outsourcing of functions

- (a) Save and except for any function that involves the decision making functions of the digital asset custodian or any interaction or direct contact with the clients, a digital asset custodian may outsource its functions to service providers, subject to compliance with the requirements set out in paragraphs 28.08 to 28.18 of the Guidelines. The board of directors of the digital asset custodian remains accountable for all outsourced functions.
- (b) A digital asset custodian is also required to provide the SC with information on outsourcing arrangements in the circumstances set out in paragraphs 28.19 and 28.20 of the Guidelines.

8. Changes requiring approval of or notification to SC

- (a) A digital asset custodian must obtain the SC's prior approval in circumstances where any proposed change to the shareholding will result in a direct or indirect change in the digital asset custodian's controller.
- (b) A digital asset custodian must notify the SC if it intends to provide custodial services for additional classes of digital assets.

9. Cessation of business operations

- (a) A digital asset custodian shall not cease its business or operations without prior engagement with the SC.
- (b) The SC may issue a direction or impose any term or condition for the purposes of ensuring the orderly cessation of the business or operations of the digital asset custodian.
- (c) A digital asset custodian must ensure that the clients continue to have uninterrupted access to their respective digital assets under its custody in the event that the digital asset custodian ceases to operate or cannot fulfil its obligation under the custodial agreement.
- (d) The cessation of business or operations of the digital asset custodian will not take effect until the SC is satisfied that all requirements stated in the securities laws, the Guidelines, relevant guidelines issued by the SC and any other relevant laws or requirements, have been fulfilled.

E. COMMENTS

The coming into force of the Guidelines has been long awaited and is undoubtedly welcomed by stakeholders in the digital assets space. The Guidelines complement the Capital Markets and Services (Prescription of Securities)(Digital Currency and Digital Token) Order 2019 and the SC's Guidelines on Recognised Markets, the latter of which, among others, set out the requirements for operators of digital asset exchanges. With the enforcement of the Guidelines, the regulatory framework for digital assets in Malaysia is now complete.

Alert prepared by Natalie Lim and Lee Ai Hsian, Partners in the Fintech Practice Group of Skrine.