Monetary Authority of Singapore

FINANCIAL SERVICES AND MARKETS ACT 2022

GUIDELINES ON LICENSING FOR DIGITAL TOKEN SERVICE PROVIDERS

TABLE OF CONTENTS

1. Purpose

1.1 The Guidelines on Licensing for Digital Token Service Providers (the "Guidelines") are intended to provide guidance on the application procedures, licensing criteria and ongoing requirements for Digital Token Service Providers under Part 9 of the Financial Services and Markets Act 2022 (the "FSM Act"). Under this, digital token service providers are defined as individuals, partnerships or Singapore corporations that are operating from a place of business in Singapore or formed or incorporated in Singapore but carry on a business of providing digital token services outside Singapore ("DTSPs").

1.2 These Guidelines should be read in conjunction with the provisions of the FSM Act, the Financial Services and Markets (Digital Token Service Provider) Regulations (the "FSM Regulations") and other relevant legislation, notices, guidelines and FAQs issued by the Monetary Authority of Singapore ("MAS").

1.3 MAS will update these Guidelines periodically to provide further guidance.

2. Licence under the FSM Act

2.1 Pursuant to section 137 of the FSM Act, any person that conducts digital token services in Singapore as defined in the First Schedule of the FSM Act is required to hold a licence unless that person is exempted. Section 137(5) of the FSM Act sets out the applicable exemptions from holding a licence.

2.2 As MAS will not be providing a transitional arrangement for DTSPs, DTSPs which are subject to a licensing requirement under section 137 of the FSM Act must suspend or cease carrying on a business of providing digital token services outside Singapore by 30 June 2025. A DTSP that contravenes the licensing requirement is guilty of an offence and would be liable to penalties set out in section 137(6) of the FSM Act.

Types of Digital Token Services

2.3 An applicant should consider whether it is providing digital token services under its business model, in accordance with the ten digital token services in the First Schedule of the FSM Act. The applicant should also consider whether its proposed activities fall within any exclusions from the scope of digital token services regulated under the FSM Act, under Part 2 of the First Schedule.

3. Admission Criteria

3.1 DTSPs are susceptible to higher money laundering, terrorism financing and proliferation financing ("ML/TF") risks due to the internet-based and cross-border nature of such services. This would result in a greater risk of such providers being engaged in or misused for illicit purposes to the detriment of Singapore's reputation. In light of these risks, MAS approaches the licensing of DTSPs in a prudent and cautious manner, and there will be extremely limited circumstances under which MAS will consider granting an applicant a DTSP licence under the FSM Act. The extremely limited circumstances include:

- The applicant has a business model that makes economic sense, and is able to demonstrate to MAS' satisfaction that it has valid reasons as to why it does not intend to carry on a business of providing digital token services in Singapore despite operating in or being formed or incorporated in Singapore;
- The applicant does not operate in a manner that is of concern to MAS and is already regulated and supervised for its compliance with relevant internationally agreed standards, such as standards established by the Financial Stability Board, the International Organisation of Securities Commissions and the Financial Action Task Force ("FATF"); and
- MAS does not have concerns with the business structure of the applicant in relation to, for example, its ability to comply with regulatory obligations.

3.2 An applicant must fully fulfil the criteria set out below and clearly demonstrate how it is able to comply with its obligations under the FSM Act as a licensee.

3.2.1 **Governance and ownership requirements** - The applicant must comply with the governance and ownership structure set out in *Appendix 1* and must be registered with ACRA.

3.2.2 **Fit and Proper** - The applicant must satisfy MAS that its sole-proprietor, partners, managers or directors and CEO, shareholders and employees, as well as the applicant itself, are fit and proper, in accordance with the Guidelines on Fit and Proper Criteria [FSG-G01]. The onus is on the applicant to ensure that the relevant persons are fit and proper to the satisfaction of MAS, rather than for MAS to show otherwise. Other than honesty, integrity and reputation, competence and capability and financial soundness, MAS would also consider other factors such as whether there is any conflict of interest and time commitment the relevant persons have for the entity in Singapore. In particular, the entity and its related group should not have any adverse reputation, particularly with regard to financial crime and sanctions compliance.

3.2.3 **Competency of Key Individuals** - The applicant must ensure that its sole-proprietor, partners, managers or executive directors and CEO have sufficient experience in operating a business in the digital token services industry, including having sufficient understanding of the regulatory framework for DTSPs in Singapore.

Where the individual will be managing a sizeable team, the sole-proprietor, partners, managers or executive directors and CEO should also have the relevant experience, competencies, and influence, to allow them to exercise

effective oversight and control over the business activities and staff.

The applicant should also consider the educational qualifications and professional certification of its key individuals.

3.2.4 **Permanent place of business or registered office** - The applicant must have a permanent place of business or registered office in Singapore. It must be an office area where the applicant's books and records can be securely held. The applicant must also appoint at least one person to be present to address any queries or complaints from customers[1], as well as inquiries/requests for information from the authorities.

3.2.5 **Base Capital** - A licence applicant must satisfy MAS that it is familiar with the base capital requirements as set out in the FSM Regulations[2] and demonstrate clearly how it will meet the requirements on an ongoing basis, as summarized in Table 3 below. In view of this obligation, the applicant must ensure that it maintains sufficient capital buffer in excess of the base capital requirement, bearing in mind the scale and scope of its operations and the potential for profit and losses. As a general rule of thumb, the base capital of the entity should be able to cover at least 6 to 12 months of the applicant's operating expenses. The applicant should also have an effective monitoring process in place to ensure that it is able to meet the base capital requirement at all times e.g. putting in place regular reporting or a specified capital buffer above the minimum requirement.

Table 1 - Base Capital Requirement

Business Type	**Base Capital Requirement**
Sole-proprietor	Maintain cash deposit of at least S$250,000 with MAS
Partnership/ Limited Liability Partnership	Total capital contribution of at least S$250,000
Corporation	Base capital of at least S$250,000

3.2.6 **Compliance Arrangements** - The applicant must have in place plans for effective compliance arrangements and ensure that it puts in adequate

[1] As set out in MAS Notice FSM-N32, licensees must appoint at least one person to be present at its permanent place of business or registered office for a minimum of 10 days a month and a minimum of eight hours on each of those days during its normal business hours, unless:

(a) it has notified all its customers in writing and in advance of any planned non-operating days that will prevent it from meeting the specified days and hours; or

(b) there are circumstances beyond the control of the licensee that could not reasonably have been foreseen that prevent it from meeting the specified days and hours.

[2] Base capital means the sum of (i) the paid-up ordinary share capital and irredeemable and non- cumulative preference share capital and (ii) any unappropriated profit or loss, less any interim loss and dividend that has been declared.

compliance resources that are commensurate with the nature, scale and complexity of its business. The minimum requirements in respect of compliance arrangements are set out in *Appendix 2*. Regardless of the setup of the compliance arrangements, the ultimate responsibility and accountability for ensuring compliance with applicable laws and regulations rests with the applicant's sole-proprietor, partners, managers or directors and CEO.

3.2.7 **Technology Risk Management** - Applicants must perform a penetration test over its proposed digital token services, remediate all high-risk findings identified, and conduct independent validation on the effectiveness of the remediation actions. This does not need to be completed prior to application but must be completed prior to the grant of licence.

3.2.8 **Audit Arrangements** - The applicant must have plans in place for adequate independent audit arrangements to regularly assess the adequacy and effectiveness of its procedures, controls, and its compliance with regulatory requirements. The audit arrangements should be commensurate with the scale, nature, and complexity of its operations. The audit may be conducted by an internal audit function within the applicant, an independent internal audit team from the head office of the applicant, or outsourced to a third-party service provider.

3.2.9 **Annual Audit Requirements** - The applicant must have in place plans to meet the annual audit requirements as set out in section 158 of the FSM Act. The auditor must be appointed at the applicant's own expense to carry out an audit of its accounts and transactions, and compliance with the relevant regulations and requirements.

3.2.10 **Letter of Responsibility and/or Letter of Undertaking** - Where appropriate, MAS may require applicants to procure a Letter of Responsibility and/or Letter of Undertaking from the applicant's majority shareholders, parent company and/or related company. The template will be provided by MAS if the application is approved.

Other Factors - MAS may also take into consideration factors such as:

3.2.11 track record and financial condition of the applicant, its holding company or related corporations, where applicable;

3.2.12 operational readiness of the applicant, including ability to comply with regulatory requirements;

3.2.13 whether the applicant has demonstrated adequate awareness of the key risks associated with its business activities and has sufficiently identified, assessed and mitigated the associated risks accordingly; and

3.2.14 whether the public interest will be served by granting a licence.

3.3 MAS considers each application on its own merits and may take into account other factors on a case-by-case basis. The criteria and considerations listed above are not meant to be exhaustive; MAS may impose additional conditions or requirements to address the unique risks posed by applicants.

3.4 The applicant should submit an application in Form 1. All applicants and licensees are required to pay the relevant fees set out in the Schedule to the FSM Regulations. Please refer to *Appendix 4* for more information on fees. Applicants should also refer to *Appendix 5* for more information on the rules of engagement for the application review process.

4. Licence Application Requirements

4.1 Applicants who have assessed that they are able to meet the admission criteria should refer to *Appendix 3* for guidance on information required as part of the licence application.

Legal Opinion for New Licence Applications

4.1.1 New applicants applying for a DTSP licence will need to submit a legal opinion from a reputable law firm together with their applications. The legal opinion should include a clear and concise summary of the applicant's business model and an assessment of whether the applicant's proposed service(s) and/or product(s) are regulated digital token services under the FSM Act.

4.1.2 In all cases, MAS reserves the right to request for a second legal opinion if the initial legal opinion is unclear.

External Auditor's Independent Assessment

4.1.3 Upon being granted an in-principle approval ("IPA"), an applicant would be required to appoint a qualified independent External Auditor to perform an independent assessment of its policies, procedures and controls in the areas of Technology and Cybersecurity risks[3].

[3] This requirement would be incorporated as an IPA condition. Please refer to Appendix 6 of the scope of assessment on Technology and Cybersecurity Risks

5. Ongoing Requirements for Licensees

5.1 A licensee is required to comply, on an ongoing basis, with all applicable requirements set out under the FSM Act, as well as other relevant legislation. Licensees are expected to put in place processes, systems, policies and procedures to ensure that they fulfil all ongoing obligations, including applications and notifications to MAS where necessary. Some of these requirements are summarised below. Please note the list is non-exhaustive and licensees should keep up-to-date with regulatory developments and may refer to MAS website for the latest requirements.

5.2 **Anti-Money Laundering and Countering the Financing of Terrorism** ("**AML/CFT**") **Requirements** - A licensee must comply with the AML/CFT requirements as set out in the Financial Services and Markets Regulations (including regulations for targeted financial sanctions), Terrorism (Suppression of Financing) Act 2002, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992, Notice on Prevention of Money Laundering and Countering the Financing of Terrorism [FSM-N27] and Notice on Reporting of Suspicious Activities & Incidents of Fraud [FSM-N28]. A licensee should also refer to the Guidelines to Notice FSM-N27 for guidance on their AML/CFT requirements.

5.3 **Periodic Returns** - A licensee must submit periodic regulatory returns in relation to its digital token activities, in accordance with the FSM Regulations. The requirements are set out in the Notice on Submission of Regulatory Returns [FSM-N29].

5.4 **Cyber Hygiene** - A licensee must comply with the cyber hygiene requirements as set out in the Notice on Cyber Hygiene [FSM-N31] and put in place appropriate safeguards to protect customer information.

5.5 **Technology Risk Management** – A licensee must comply with the Notice on Technology Risk Management [FSM-N30] and refer to the Guidelines on Risk Management Practices – Technology Risk for guidance on technology risk management requirements.

5.6 **Business Conduct** - A licensee must comply with business conduct requirements in the FSM Act, the FSM Regulations and the Notice on Conduct [FSM-N32]. These obligations include record of transactions, issuance of receipts, display of exchange rate and fees, and notification of normal business hours. Licensees must also ensure that they comply with all prohibitions and restrictions, including prohibited business activities.

5.7 **Disclosures and Communications** - A licensee must make accurate representation on the scope of its licence and provide the disclosures set out in the Notice on Disclosures and Communications [FSM-N33] where applicable to its business. A licensee should also ensure that customers receive timely updates regarding any material changes to the disclosures.

5.8 **Annual Audit Requirements** - A licensee must, on an annual basis, appoint an auditor to carry out an audit of its accounts and transactions, and compliance with regulations and requirements. The licensee must ensure that the auditor submits a report to MAS in **Form 3**.

Appendix 1

A1 Governance and Ownership Requirements

Table A1 - Governance/Ownership Requirements for Licensees

Entity Type	Governance/Ownership Requirements
Individuals	Not applicable.
Partnership or Limited Liability Partnership (LLP)	• At least one partner or manager must be resident in Singapore.
Corporations	• At least one executive director must be resident in Singapore.

Appendix 2

A2 Minimum Compliance Arrangements

The applicant should ensure that it has effective compliance arrangements and adequate compliance resources, commensurate with the scale, nature and complexity of its operations. This may take the form of:

- An **independent compliance function** - The applicant should put in place an independent compliance function in Singapore with staff who are suitably qualified in the areas relevant to its business activities. Compliance staff may perform other non-conflicting and complementary roles such as that of an in-house legal counsel.
- **Compliance support from holding company or overseas related entity** - The applicant may obtain compliance support from an independent and dedicated compliance team at its holding company, or at an overseas related entity, provided that it is able to demonstrate that there is adequate oversight by the applicant's compliance officer, sole-proprietor, partners, managers or directors and CEO and other senior management.

The applicant must also develop appropriate compliance management arrangements, including at least, **the appointment of a suitably qualified compliance officer at the management level**. This individual should be **based in Singapore**. This individual should have sufficient expertise in the areas relevant to the business activities, and authority to oversee the compliance function of the applicant, although he may be assisted by other staff in day-to-day operations.

The applicant should also put in place proper governance structure to oversee compliance and AML/CFT issues (including those in relation to targeted financial sanctions). Depending on the scale of the business and its group structure, the applicant can consider having the compliance officer regularly reporting compliance and AML/CFT issues to the board or a board committee and for decision on matters which is beyond the authority of the compliance officer.

The applicant should note that regardless of the arrangement chosen, the sole-proprietor, partners, managers or directors and CEO of the applicant are ultimately responsible for all compliance and regulatory matters and must maintain adequate oversight over the arrangements.

Accordingly, senior management and compliance officer of the applicant are expected to be able to demonstrate their sufficient understanding of the compliance and ML/FT risks which the applicant faces in relation to its business activities and the measures which they have put in place to effectively manage the risks.

Appendix 3

A3 Guidance on Information required for Licence Applications

The applicant should ensure that it fully meets the admission criteria, and has ensured that the application is complete, free of errors and inconsistencies, and accompanied by the requisite supporting documents stated in the application form.

Information Required in Proposed Business Plan

In particular, it should include the following information in its proposed business plan:

The applicant should provide a clear description of its business model and plans, which are supported by the professional experience and expertise of the proposed management team. The business plan should illustrate compliance with the FSM Act and relevant subsidiary legislation, and include the information below:

- Jurisdictions serviced, including evidence that the applicant is licensed to operate in and supervised for its compliance with relevant internationally agreed standards, such as standards established by the Financial Stability Board, the International Organisation of Securities Commissions, and FATF by all the relevant supervisors in the jurisdictions where it is providing digital token services.

- Profile of target clientele.

- Proposed products and services. The applicant should indicate clearly its assessment of which digital token service(s) will be conducted at each stage of the transaction process. Where the applicant intends to provide more than one type of digital token service, the applicant should provide a separate assessment for each type of digital token service.

- Reason(s) on why it does not intend to carry on a business of providing digital token services in Singapore despite operating in or being formed or incorporated in Singapore.

- Detailed funds flow plan and channels, including transaction and/or process flow diagrams. If there is more than one product or service, or more than one type of transaction and/or process flow, one diagram should be provided for each flow. The diagrams should:

    - Describe the beginning to end of a typical transaction, starting from the sources of funds that the applicant will accept (e.g. bank transfers, cash, cards) until where the obligation to the customer is fully discharged.

    - Illustrate both the interactions between the customer and the applicant and the flow of funds.

    - Have timelines indicated, including service level agreements with third parties, and payment and settlement cycles, where applicable.

    - Highlight where it uses innovative technology (e.g. use or offering of digital

tokens, distributed ledger technology) or a different manner of delivering products or services from that commonly seen in the market.

- Include all third parties involved (e.g. other digital token service providers, banking partners, intermediaries, other agents) and show their roles in the process.

- Implementation plans, including the anticipated timeline for business/product launch, as well as systems, processes, and third parties that will perform a key role in its operations.

- Whether the digital token services are incidental to, or bundled with, any other products or services offered by the applicant.

- Brief description of any other activities regulated by MAS that it conducts or intends to conduct (e.g. financial advisory, dealing in securities etc.).

- Brief description of any exempted and unregulated activities that it currently conducts or intends to conduct.

- For applicants that are part of a global digital token services group:

  - Role of the applicant within the group, including the functions or services that it will receive and/or provide to related corporations within the group, if any. Where available, the applicant should provide an estimate of the level of resources (in terms of headcount and time spent) in the other related corporations that will support the operations in Singapore.

  - Confirmation that all its entities are adequately licensed/registered, with the licensing/registration details of each entity. Applicants should provide copy of its licence/ certification of registration or information of its licensing/registration status on the regulators' websites. Applicants should disclose any regulatory enforcement action/investigation which any of its entities may have been a party to.

- Holistic risk assessment of all the digital tokens and digital token services (e.g. exchange platform, custody) that they intend to support or provide, including its token listing governance process. The applicant should provide a full list of digital tokens supported and indicate its assessment of the nature of the token under MAS' regulatory framework (e.g. if it is a security token or a payment token).

- Information on its consumer access measures and business conduct measures in place to maintain access and operational controls to customers' digital tokens in Singapore, daily reconciliation of customers' accounts and provision of monthly account statements to customers, risk management controls (control of movement of customers' assets), disclosures to customers.

Legal opinion

Applicants are required to provide a legal opinion from a reputable law firm on the regulated digital token services to be offered given the applicant's proposed business model. The legal opinion should include (but not be limited to) the following:

- A clear and concise summary of the applicant's business model, as well as each of the service(s) and product(s) the applicant intends to offer (including asset/fund flows and parties involved for each service/product where applicable).

- An assessment of whether the proposed service(s) or product(s) are regulated digital token services under the FSM Act. The assessment should include a detailed and comprehensive analysis of how each regulated digital token service is or is not applicable to each proposed service or product. The assessment should also consider all relevant Legislation, Notices, Guidelines, Circulars and FAQs.

- If any of the proposed service(s) or product(s) are assessed to be exempted or excluded from regulation, a detailed explanation of how the relevant exemption or exclusion applies.

- An acknowledgement that the legal opinion will be disclosed to the Authority.

Information Required on Compliance, Risk Management, Systems & Controls

Technology risk management

The applicant should set out its framework for assessing and managing technology risks, and implement measures to protect customer data, transactions and systems that are commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services. The applicant should refer to the Notice on Technology Risk Management [FSM-N30], Notice on Cyber Hygiene [FSM-N31], and Guidelines on Risk Management Practices – Technology Risk for guidance on IT risk management principles and supervisory expectations.

Compliance and audit

The applicant should provide the following information and documents that are in line with the nature of the proposed business model:

- AML/CFT policies and procedures that demonstrate compliance with MAS Notice FSM-N27, as well as the relevant targeted financial sanctions requirements. This should include the framework for assessing and maintaining oversight of agents and third-party partners (local and overseas).

- Enterprise-wide money-laundering/terrorism financing/proliferation financing risk assessment ("EWRA"). Applicant should also include an assessment on the tax evasion risk in the EWRA.

- AML/CFT governance, escalation and reporting arrangements. This should include details of the involvement of the sole-proprietor, partners, managers or directors and CEO and other senior management in the oversight and resolution of AML/CFT issues that may arise in the course of the licensee's business.

- Implementation plans of compliance management arrangements, including the processes that have been rolled out, and systems that will be used.

- Name and Curriculum Vitae ("CV") of the compliance officer, including details of any formal compliance accreditation e.g. ACAMS, IBF accreditation.

- Staffing arrangements and reporting lines for the compliance function if it is not already provided as part of the organisational chart. This should include details on all outsourced compliance functions, including where the outsourced provider and team is located, relationship between the applicant and the outsourced provider (e.g. vendor, parent company), licensing/registration status of the outsourced provider, and oversight arrangements.

- Internal and external audit arrangements.

Shareholding Chart

- The applicant should provide the complete shareholding chart (up to the ultimate controller(s)) who are natural person(s).
- If the applicant does not have any 20% controller, the applicant will have to provide a written confirmation.

Appendix 4

A4 Annual Licence Fees

Under section 140 of the FSM Act, licence fees are to be paid annually, as set out in the Schedule to the FSM Regulations. All licence fees paid are non-refundable.

The licensee should have a GIRO arrangement with MAS for the payment of licence fees on an annual basis. The licensee should ensure that its GIRO arrangement details are updated and there are sufficient funds in its bank account on the deduction date stated on the fee advice.

Pro-rated licence fee for new licence holders

For new licensees that are not licensed on 1 January of the year, the licence fee payable for the first calendar year of it being licensed is computed based on the pro-rated amount of the fixed annual licence fee for the period from the licence issue date to 31 December of the same year. Example 1 shows the computation of the first year's licence fee.

Example 1

A company is issued a DTSP licence on 1 December 2025.

Licence Issuance Date	1 December 2021
Pro-rated fee payable for the first calendar year (for the period 1 December 2025 - 31 December 2025 i.e. 31 days)	(31/365) * $10,000 = $849.32
Annual licence fee payable for subsequent calendar years	$10,000

Appendix 5

A5 Rules of Engagement for the Application Review Process

Initial Review and Information Request

The review process of an application begins when a case officer is assigned and upon complete submission of all information and documents as required. Depending on the volume of applications received, the case assignment may not take place immediately upon MAS' receipt of an application. Following a case assignment, the case officer will reach out to the applicant to inform the applicant of the necessary next steps, which may include an opening meeting.

The case officer will check the complete set of submitted documents, and this typically forms the initial round of information requests that the applicant will receive. The case officer will also make an initial review of the applicant's business model. In the course of the review process, there may be multiple rounds of requests for information and clarifications, depending on the completeness of the responses submitted by the applicant.

The applicant should always ensure that the application meets the admission criteria as set out in these Guidelines, and contains the necessary information as required in Appendix 3 of these Guidelines before submitting the application. Where submissions are assessed as grossly incomplete or significantly deficient, MAS reserves the right to reject the applications. The applicant is also expected to have a contact person available at all times to follow up on these information requests and provide an adequate response on a timely basis. Should there be any changes to the contact person, the applicant is expected to inform MAS in a timely manner.

It is crucial that applicants proactively and fully disclose all material information without any suppression to the case officer in a timely manner. In situations where applicants are found to have intentionally obfuscated, hidden or delayed their disclosures to the MAS without good reason, these will be considered as significant deficiencies. The applicant is reminded that it must use reasonable care to ensure that information and document provided to MAS is not false or misleading. An individual who contravenes section 176(1) or 176(3) of the FSM Act may be guilty of an offence and liable on conviction to a fine or imprisonment.

Timeliness and Quality of Responses

MAS typically provides the applicant with a deadline to respond to requests for information. If the applicant fails to respond within the stipulated time, MAS will deem the application to be withdrawn. Should the applicant require additional time to prepare the response, the applicant should inform the case officer in advance.

The applicant must also balance the time needed to provide an adequate and comprehensive response against rushing out a hasty response in the hopes of speeding up the review. Failing to provide a satisfactory and comprehensive response

will be assessed as deficiencies that will result in an unfavorable consideration of the application.

Interview

The case officer will typically arrange for an interview with the applicant's key management personnel and/or the compliance officer. All representatives of the applicant are expected to treat their interactions with the case officer seriously. The purpose of the interview is for the applicant to explain how it intends to manage the business and risks in compliance with regulatory requirements. Consultants, external legal counsel, and other third parties are not permitted to attend the interview. This is because the applicant remains responsible for meeting its regulatory obligations, even if it outsources any of its functions.

Potential grounds for a case officer to form a reasonable basis that the applicant will not be able to discharge its obligations as a licensed entity adequately include, but are not limited to the following:

- Not turning up for the interview without a valid reason;
- Not being able to address questions clearly during the interview; or
- Verbally abusing the case officer.

If there are material changes to the application after the interview but before there is an application outcome, the case officer may arrange for additional interview(s) with the applicant. Examples of such changes include any change in appointment of an applicant's key personnel, or any change in the applicant's business model.

MAS' Review Process

Case officers have an obligation to conduct a comprehensive assessment of the applications. Even at the application stage, the aim of an applicant is to be licensed, and therefore be subject to ongoing supervision and oversight, as per the regulatory regime. The case officer will review the application in this context and expect the applicant to conduct itself as if it were already a regulated financial institution. Applicants who fail to do so will be assessed as potentially significant deficiencies, which could result in a rejection of the application.

<u>Placing Applications On-hold</u>

If there are any changes to the information provided in the application after submission, MAS should be notified immediately. In cases of significant/major changes to the application, applicants may wish to consider withdrawing their application and reapplying after the changes have been completed in view that the application will not be ready for review until then.

MAS reserves the right to place any application that is assessed to be insufficiently ready for review, to be on-hold for six months in the event of an applicant's major

corporate restructuring, substantial changes to key management personnel[4][10], or material variations in the business model/activities, at any point during the review process. While such significant changes could be unforeseen on the applicant's part, the on-hold period allows for resources to be redirected away from such incomplete applications, to ensure fairness to all other ready applicants in the queue.

During this on-hold period, the onus is on applicant to ensure timely resolution/completion of all necessary changes and to provide MAS with the relevant documentation to be assessed at the end of the on-hold period. The default on-hold period is six months and is not extendable. If the significant change is not completed within the on-hold period, the application will be assessed to be insufficiently ready for review and the applicant should consider withdrawing the application.

Withdrawal of applications

Applicants have the right to withdraw its application at any time. After MAS' review, an applicant with fundamental concerns that cannot be adequately addressed within a reasonable timeframe, or whose application has been assessed to be significantly deficient, may also be recommended to withdraw the application. The applicant should be aware that if the case officer has made such an assessment, the case officer would have determined that other applicants in similar positions have not received approvals. Robust controls are in place to ensure that case officers conduct a fair, objective, and verifiable assessment. Each application and its supporting documents are rigorously reviewed by a team comprising the case officer, supervising officers, as well as by the reviewing and approving authorities. As such, applicants should treat the review process and its outcomes seriously.

If the applicant intends to resubmit the application, the applicant needs to ensure that it has fully addressed all concerns and deficiencies before doing so. Re-submission of an application without remediation of concerns previously raised by MAS is likely to result in rejection.

[4] In relation to applications being placed on-hold, significant changes to key management personnel mainly refer to changes related to the key C-suite positions such as Chief Executive Officers, Chief Financial Officers, Chief Risk Officers and Chief Compliance Officers. However, applicants should also assess and highlight if there are other role changes that should be considered as key management personnel based on criticality to their business models and importance of reporting lines.

Appendix 6

A6 External Auditor Independent Assessment

A. Technology & Cybersecurity Risks:
(Required for applicants upon the grant of an in-principal approval)

1) Criteria for External Auditor Appointed to Perform the Independent Assessment of Technology and Cybersecurity risks

The External Auditor appointed by the applicant to conduct the independent assessment should meet the following criteria:

Criteria	Minimum Requirements
1) Qualifications, credentials, and track record of the External Auditor and its lead engagement partner / engagement leader	a) The External Auditor should be a company, firm or limited liability partnership approved or deemed to be approved as an accounting corporation, accounting firm or accounting limited liability partnership, respectively, under the Accountants Act 2004. b) The External Auditor, as well as its lead engagement partner/ engagement leader[5], must have made: • at least one report in respect of a statutory audit pursuant to MAS regulations on a financial institution regulated or authorised by MAS, or • at least one independent review/ assessment in the area of technology and cybersecurity risks on a financial institution regulated or authorised by MAS.
2) Independence	a) The External Auditor should be independent from the applicant, its group or group companies. b) In the provision of its services for purpose of conducting the independent assessment for the applicant, the External Auditor must satisfy itself that there are no conflicts of interest arising from its ongoing business relationships with the applicant, its group or group companies, up to the conclusion of its engagement.

2) Scope of Assessment

The following sets out **Technology and Cybersecurity Risks** areas to be assessed by an Independent External Auditor, that will be imposed as in-principal approval (IPA) condition.

[5] The engagement leader should be of sufficient seniority, and has adequate experience and expertise in the area of technology and cybersecurity risks (tech risk). The onus is on the applicant to ensure that it appoints a suitably qualified independent External Auditor to perform an independent assessment of its policies, procedures and controls on tech risk.

I. Cyber Hygiene –

a. Taking into consideration the applicant's proposed business model, products, services, funds flows and delivery channels,

   i. identify any gaps against relevant regulatory requirements set out in MAS Notice FSM-N31 Cyber Hygiene; and
   ii. highlight any areas of improvements required to mitigate cyber hygiene risks.

II. Data Loss Prevention –

a. Review and assess the applicant's proposed IPPCs on data loss prevention in the following areas:

   i. Protection of sensitive data (including customer data) during transmission and storage;
   ii. Detection and prevention of unauthorised access or disclosure (including communication, transfer and storage) of sensitive data (including customer information); and
   iii. Protection of cryptographic keys for custodial wallet.

b. Taking into consideration the applicant's proposed business model, products, services, funds flows and delivery channels,

   iv. identify any gaps against applicable technology risk management regulatory requirements set out including but not limited to MAS Notice FSM-N30 Notice on Technology Risk Management and section 11 of the Guidelines on Technology Risk Management; and
   v. highlight any areas of improvements required to mitigate technology risks posed by its proposed business model.

III. Penetration Testing –

a. Review and assess the applicant's proposed IPPCs on penetration testing systems, including:

   i. frequency of the penetration testing that is determined based on factors such as system criticality and the system's exposure to cyber risks. For systems that are directly accessible from the Internet, the applicant should conduct penetration testing to validate the adequacy of the security controls at least once annually or whenever these systems undergo major changes or updates; and
   ii. Service Level Agreements ("SLAs") to rectify penetration testing findings that is commensurate with the associated risk levels.

b. Review and assess whether the penetration test(s) performed (within the last 12 months) on the applicant's proposed online financial service(s) are relevant and adequate to identify critical security weaknesses.

c. Taking into consideration the applicant's proposed business model, products, services, funds flows and delivery channels,

   i. identify any gaps against applicable technology risk management regulatory expectations set out including but not limited to section 13.2 of the Guidelines on Technology Risk Management; and

ii. highlight any areas of improvements required to mitigate technology risks posed by its proposed business model.

IV. Digital Wallet and Smart Contracts –

a. Review the applicant's proposed IPPCs and assess whether the proposed IPPCs include the following controls that are commensurate with the applicant's proposed business model, products, services, funds flows and delivery channels:

i. Adherence to security-by-design principles (including proper access control, thorough testing, regular updates to stable versions, static and dynamic code analysis) throughout its system development life cycle for its proposed system(s) and smart contracts, if relevant;
ii. Development of smart contracts, including controls to ensure smart contracts are secure from cyber threats and vulnerabilities by having secure development, DevSecOps, and testing, to prevent unauthorised access, data breaches, and exploitation of security flaws;
iii. Controls to ensure high availability of critical systems, as well as recovery of system(s) and business resumption priorities (including root cause and impact analysis) to ensure swift recovery strategy for such system(s);
iv. Adoption of techniques, such as multi-party computation and threshold signature schemes, to secure custodial wallets;
v. Implementation of network isolation between the custodial wallet systems and other information systems/ Internet to prevent unauthorised connections; and
vi. Segregation of cryptographic key components for custodial wallets to ensure that no single individual or system has access to the complete key at any time (i.e. adhere to the "never alone" principle by requiring at least two authorised personnel to coordinate and approve key management operations).