



**Response to Feedback
Received on Proposed
Regulatory Approach,
Regulations and Notices for
Digital Token Service
Providers issued under the
Financial Services and
Markets Act 2022**



Contents

1. Preface	3
2. Regulatory approach for Digital Token Service Providers	4
3. Financial Services and Markets Regulations: Overview and requirements for licensees	5
4. Financial Services and Markets Notices: Overview	10
5. Financial Services and Markets Notices: AML/CFT requirements for Licensees	11
6. Notices on reporting requirements, technology risk management and cyber hygiene	16
7. Notices on Conduct and Disclosures and communications	19
8. Guidelines applicable to licensees	21
Annex A	23
Annex B	25



1. Preface

- 1.1. On 4 October 2024, the Monetary Authority of Singapore (“MAS”) issued a consultation paper on the proposed regulatory approach, regulations, notices and guidelines for digital token service providers issued under the Financial Services and Markets Act 2022 (“FSM Act”) (the “consultation paper”). 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 (“DT”) services outside Singapore (“DTSPs”).
- 1.2. The consultation period closed on 4 November 2024, and MAS would like to thank all respondents for their contributions. MAS has considered carefully the feedback received and incorporated them where justified and appropriate. Comments that are of a wider interest, together with MAS’ responses, are set out below. The list of respondents and their full submissions are provided in the Annexes at the end of this paper.
- 1.3. For further queries, please write in to MAS at AMLCFT@mas.gov.sg.



2. Regulatory approach for Digital Token Service Providers

- 2.1. DTSPs may be more susceptible to money laundering or terrorism financing (“ML/TF”) risks due to the internet-based and cross-border nature of such services. This would result in a greater risk of DTSPs being engaged in or misused for illicit purposes to the detriment of Singapore’s reputation.
- 2.2. In light of the risks set out above, as set out in the consultation paper, MAS will approach the licensing of DTSPs in a prudent and cautious manner and there will be extremely limited circumstances¹ under which MAS will consider granting an applicant a licence under section 138 of the FSM Act (a “DTSP licence”).
- 2.3. In addition, as set out in Paragraph 2.8 of the consultation paper, MAS will not be providing a transitional arrangement for DTSPs. Hence, **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 DT services outside Singapore by 30 June 2025**, when Part 9 of the FSM Act, the First and Second Schedules to the FSM Act, and other relevant miscellaneous or consequential amendments in the FSM Act (collectively, the “DTSP Provisions”) come into force. 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.

¹ As MAS had broadly set out under Paragraph 2.4 of the consultation paper, MAS will take into account whether the applicant meets the criteria set out below:

- (a) 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 DT services in Singapore despite operating in or being formed or incorporated in Singapore;
- (b) 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 FATF by all the relevant supervisors in the jurisdictions that they provide DT services outside of Singapore. For example, the applicant should be able to demonstrate that its proposed provision of DT services is in compliance with the relevant internationally agreed standards;
- (c) MAS does not have concerns with the business structure of the applicant in relation to, for example, the ability of the applicant to comply with regulatory obligations; and
- (d) Any other criteria that may be relevant to the application (or applicant), as determined by MAS.



3. Financial Services and Markets Regulations: Overview and requirements for licensees

Control of Provision of Digital Token Services

- 3.1. MAS proposed that no transitional arrangement will be provided for DTSPs. As set out in the consultation paper, to give the industry sufficient notice, we will publish the commencement notification for the FSM Act as well as all finalised versions of the subsidiary legislation, notices and guidelines at least four weeks before the date of commencement of the DTSP Provisions (the “four-week commencement notification period”).
- 3.2. Under the regulations which MAS will prescribe for the purpose of Part 9 of the FSM Act (“FSM Regulations”), MAS has set out the forms, documents and fees which would be applicable to DTSPs who wish to apply for a licence under section 138(1) of the FSM Act. MAS has also set out the situations where a DTSP licence will lapse in the FSM Regulations.
- 3.3. Several respondents raised concerns that the four-week commencement notification period proposed by MAS would be insufficient time for applicants to prepare a licence application and for MAS to review the application. Respondents suggested MAS to consider providing a transitional period, a temporary exemption to allow applicants to continue providing DT services while their licence applications are under review, or to have an expedited review process for simple business models or applicants that are regulated in other jurisdictions.
- 3.4. Several respondents also suggested to adopt a tiered fee structure for licence application fees and annual licence fees (“DTSP licence fees”), commensurate with an applicant’s or licensee’s size and scope of its business operations. One respondent also sought clarifications on whether the annual licence fees payable by licensees would differ based on the number of DT services provided.
- 3.5. One of the respondents also sought clarifications on the scope of the FSM Act, specifically whether DTSPs that only house its senior management and directors and/or are set up solely for the purposes of establishing a Singapore tax residency would require a DTSP licence.
- 3.6. Several respondents also sought clarifications on the reasons for the inclusion of requirements beyond Anti-Money Laundering and Countering the Financing of Terrorism (“AML/CFT”), such as



technology risk related requirements, and the actions that MAS will take against unlicensed entities conducting regulated activities under the FSM Act.

MAS' Response

- 3.7. As set out in the consultation paper and Part 2 above, MAS is cautious about DTSPs as they are more susceptible to ML/TF risks due to the internet-based and cross-border nature of DT services. In addition, given that DTSPs carry on a business of providing DT services outside Singapore and hence have little to no nexus to Singapore in relation to the provision of DT services, the key risk DTSPs pose to Singapore would be reputational risk should they engage in or be misused for illicit purposes.
- 3.8. Therefore, MAS would like to reiterate that a DTSP licence will only be granted under extremely limited circumstances. Hence, MAS maintains our position that no transitional period will be provided. Instead, MAS will provide the four-week commencement notification period for DTSPs to suspend or cease the provision of all DT services by 30 June 2025.
- 3.9. In relation to DTSP licence fees, the proposed DTSP licence fees are structured similarly to the licence application fees and annual licence fees applied to payment service providers who provide digital payment token services ("DPTSPs"), where the fees are fixed regardless of the size and scope of the DPTSP's business operations. In particular, all licensees would be subject to an annual licence fee of \$10,000, regardless of the number of DT services which it provides. In this regard, MAS has maintained the proposed DTSP licence fees.
- 3.10. Regarding the scope of Part 9 of the FSM Act, DTSPs are (i) individuals or partnerships that are operating from a place of business in Singapore or (ii) Singapore corporations, whether from Singapore or elsewhere, that are carrying on a business of providing DT services outside Singapore, as set out in section 137 of the FSM Act. In determining whether a DTSP is "carrying on a business of providing DT services outside Singapore", factors such as whether the DTSP's front-office functions (e.g., sales, business development) or customers are located outside Singapore etc., would be relevant.
- 3.11. In respect of the inclusion of technology risk management and cyber hygiene requirements, as highlighted in the consultation paper, licensees' ability to execute DT services are dependent on the underlying distributed ledger technology and other service providers in the network. As technology related threats and vulnerabilities such as cyberattacks and system outages could significantly



impact and disrupt the licensees' provision of DT services, it would be important for licensees to implement controls to manage the technology risks that may arise in their course of business.

Financial requirements

- 3.12. Under the FSM Regulations, minimum initial and ongoing financial requirements were proposed for licensees to ensure that they are at all times sufficiently resourced to conduct the DT services they are authorised to conduct under their licence.
- 3.13. A few respondents highlighted that it would be challenging for smaller companies and startups to comply with the initial and ongoing financial requirements, and proposed that MAS should impose a tiered-capital structure or levy capital requirements on a progressive basis.

MAS' Response

- 3.14. As set out in the consultation paper, one of the key objectives of the minimum initial and ongoing financial requirements is for licensees to demonstrate their commitment to maintain a meaningful presence in Singapore. Therefore, MAS will maintain the minimum initial and ongoing financial requirements of \$250,000 in base capital, total capital contribution and cash deposit in the case of a company, partnership or limited liability partnership and individual respectively.

Business Conduct

- 3.15. MAS had consulted on the FSM Regulations that sets requirements relating to the approval of the chief executive officer ("CEO"), directors, partners or managers of a licensee. The FSM Regulations also sets out requirements relating to a report of an audit on licensees.
- 3.16. Respondents were generally supportive of the above proposed requirements. Several respondents suggested (i) explicitly requiring sector-specific qualifications for the CEO, directors, partners and managers, such as experience in financial services, digital assets, and risk management, as well as (ii) incorporating risk management responsibilities, especially those related to cybersecurity, operational resilience, and AML/CFT obligations.



- 3.17. A few sought clarifications on whether it was mandatory for licensees to have a compliance officer at the management level and the difference between the requirements set out in Paragraph 2.9(e) of the consultation paper and the compliance requirements in section 18 in the proposed Notice to DTSPs on Prevention of Money-Laundering and Countering the Financing of Terrorism (“FSM-N27 Notice”), which states that licensees must develop appropriate compliance management arrangements and ensure that its compliance function has adequate resources and timely access to information required to discharge its responsibilities.
- 3.18. In relation to the proposed audit requirements, respondents were generally supportive, and suggested for additional requirements to be included, such as: (i) mandating additional risk-based internal audits; (ii) mandating the reporting of significant audit findings to customers via the annual report or website; and (iii) establishing guidelines on the preferred format, structure and considerations to include in audit reports. A few respondents also requested for MAS to consider taking a tiered approach over the frequency of audits conducted commensurate to the size and risk profile of the licensee.

MAS’ Response

- 3.19. MAS will set out guidance on the competencies of the CEO, directors, partners and managers of the licensee in the Guidelines on Licensing for DTSPs. Competency requirements include having sufficient experience in operating a DTSP business as well as having sufficient understanding of the regulatory framework for DTSPs in Singapore. In addition, the Guidelines on Licensing for DTSPs will set out MAS’ expectations of applicants in managing key risks associated with its business activities, which MAS will consider when processing licence applications.
- 3.20. In relation to licensees’ compliance arrangements, MAS would like to highlight that licensees must have appropriate compliance management arrangements. The Guidelines on Licensing for DTSPs will set out MAS’ expectations for the compliance arrangements to be commensurate with the scale, nature, and complexity of their operations. Such arrangements may take the form of:
- an independent compliance function in Singapore; or
 - compliance support from its holding company or overseas related entity.
- 3.21. Regardless of the form of the compliance arrangement, a licensee is required under FSM-N27 Notice to appoint a suitably qualified compliance officer at the management level. MAS expects this



individual to be based in Singapore, and this expectation will be set out in the Guidelines on Licensing for DTSPs.

- 3.22. Regarding audit requirements, a licensee is required to appoint an auditor to conduct an audit of the transactions in relation to the DT services provided by the licensee, and submit the audit report to MAS annually. As part of MAS' supervision of the licensee, MAS would take into consideration the findings of the audit report and may require an auditor to carry out additional duties, such as enlarging the scope of audit or carry out any other examination, as set out in sections 158(5) of the FSM Act.
- 3.23. In addition to audits, licensees must maintain an audit function that is adequately resourced and independent, and be able to regularly assess the effectiveness of the licensee's internal policies, procedures and controls, and its compliance with regulatory requirements. These requirements have been set out under Paragraph 18.13 of the FSM-N27 Notice.



4. Financial Services and Markets Notices: Overview

- 4.1. In addition to the FSM Regulations, MAS has also proposed to issue notices and guidelines for the purposes of the commencement of the DTSP Provisions, and they will come into force on the commencement of the DTSP Provisions.
- 4.2. A respondent sought clarifications on the applicability of the FSM Act to individuals who are located in Singapore but are (i) providing DT services to overseas companies, or (ii) working for overseas companies that provide DT services outside of Singapore.
- 4.3. Another respondent suggested for less onerous requirements to be placed on individuals, due to the operational constraints that individuals may have, compared to entities.

MAS' Response

- 4.4. As set out in section 137(1) of the FSM Act, all individuals who from a place of business in Singapore carry on a business of providing DT services outside Singapore will require a DTSP licence, unless the individual falls within one of the categories of persons in section 137(5) of the FSM Act. In this regard, an individual attracts a licensing requirement under section 137(1) of the FSM Act if he or she is located in Singapore and is carrying on a business of providing DT services to persons (i.e. individuals and non-individuals) outside of Singapore. However, where an individual is an employee of a foreign incorporated company that provides DT services outside Singapore, work done by the individual as part of his or her employment with the foreign-incorporated company would not, in itself, attract a licensing requirement under section 137(1) of the FSM Act.
- 4.5. Regarding requirements placed on individuals, given that DT services provided by DTSPs are of higher ML/TF risks and exposes Singapore to potential reputational risk as DTSPs are operating from a place of business in Singapore or formed or incorporated in Singapore but carry on a business of DT services outside of Singapore, MAS will require all DTSPs, whether they are individuals or non-individuals, to obtain a DTSP licence unless the DTSP falls within one of the categories in section 137(5) of the FSM Act.



5. Financial Services and Markets Notices: AML/CFT requirements for Licensees

Existing Customers

- 5.1. Under the proposed FSM-N27 Notice, licensees are to perform customer due diligence (“CDD”) measures as required by Paragraphs 6, 7 and 8 of the proposed FSM-N27 Notice for all customers with whom it had established business relations with prior to obtaining its DTSP licence, and who continue to be its customers upon obtaining its DTSP licence (such customers being “Pre-Licence Customers”) (“the Requirement”).
- 5.2. Respondents were generally supportive of the Requirement. Several respondents sought clarifications on whether MAS would prescribe the timelines for licensees to complete the required CDD measures by.
- 5.3. A respondent also sought clarifications on requirements pertaining to subsequent revisions of CDD requirements, such as whether documentation from initial CDD can be reused if it remains valid and current, and situations in which updates to the documentation are expected.

MAS’ Response

- 5.4. For the Requirement, MAS will not prescribe any baseline timelines in the FSM-N27 Notice to complete the required CDD measures by, and will determine the timeline on a case-by-case basis at the point of licensing, which will take into consideration factors such as the licensee’s customer risk profile.
- 5.5. In relation to actions expected from licensees for subsequent revisions of CDD requirements, licensees should have internal processes to assess the measures they need to put in place to comply with the revisions. MAS will not prescribe situations where licensees must update the initial CDD for existing customers in the FSM-N27 Notice as this would primarily be dependent on the what the subsequent revisions of CDD requirements relate to. We will, however, include a list of non-exhaustive considerations which licensees should include as part of their assessment within the Guidelines to the FSM-N27 Notice.



Reliance on Third Parties

- 5.6. Under the proposed FSM-N27 Notice, it was proposed for licensees to be allowed to rely on third parties to perform CDD measures as required by Paragraphs 6, 7 and 8 of the proposed FSM-N27 Notice if they comply with several key requirements. In addition, it was also proposed for (i) licensees, (ii) financial institutions which are holders of a payment services licence under the Payments Services Act (“PS Act”) (“licensed payment service providers”), and (iii) financial institutions holding an equivalent licence to a payment services licence under the PS Act or a digital token services licence under the FSM Act, and are supervised by a foreign authority for compliance with AML/CFT requirements, to be excluded from the definition of a “third party”² under the proposed FSM-N27 Notice.
- 5.7. Respondents were generally supportive of the proposed third party reliance requirements and the exclusion of licensees, licensed payment service providers, and financial institutions holding an equivalent licence to a payment services licence under the PS Act or a digital token services licence under the FSM Act, and supervised by a foreign authority for compliance with AML/CFT requirements from the definition of “third party” in the FSM-N27 Notice.
- 5.8. However, a respondent suggested to allow licensees to rely on licensed payment service providers if they are able to meet specific criteria related to AML/CFT and demonstrate robust compliance practices. A few respondents were also of the view that licensees should be allowed to place reliance on licensed payment service providers which are supervised by a foreign authority for compliance with AML/CFT requirements consistent with FATF standards.
- 5.9. Several respondents also suggested for additional requirements to be included, such as onboarding and due diligence checks to be conducted on the third party providers.

MAS’ Response

- 5.10. As set out in the consultation paper, due to the uneven level of AML/CFT controls across the payment sector in Singapore and globally, MAS maintains our position of excluding licensed payment service providers and financial institutions holding an equivalent licence and supervised by

² For the avoidance of doubt, the definition of a “third party” would not exclude those who are subject to and supervised by a foreign authority for compliance with AML/CFT requirements and also hold other types of financial services licenses (besides licences equivalent to a payment services license under the PS Act or a digital token service provider license under the FSM Act).



a foreign authority for compliance with AML/CFT requirements, from the definition of “third party” in the FSM-N27 Notice that licensees can rely on to perform CDD measures.

- 5.11. In relation to requirements for third party reliance, licensees are indeed expected to establish internal processes for its assessment and determination of whether to rely on a third party to conduct CDD, including the due diligence checks to conduct over the third party.

Correspondent Account Services

- 5.12. Under the proposed FSM-N27 Notice, it is proposed for licensees who engage in the provision of correspondent account services to perform several risk mitigation measures to ensure that it has adequately addressed ML/TF risks arising from this provision of services.

- 5.13. Respondents were generally supportive of the requirements that licensees must comply with when providing correspondent account services. However, several respondents requested for additional guidance on licensees’ assessment of the suitability of the respondent/correspondent financial institution that is involved in correspondent account services, such as factors which licensees and their senior management should consider during evaluations, and relevant documentation templates.

MAS’ Response

- 5.14. Licensees are required to establish its internal processes for provision of correspondent account services, including the considerations prior to conducting these services. MAS will include a list of non-exhaustive factors in the Guidelines to the FSM-N27 Notice which licensees may consider when assessing the suitability of the respondent/correspondent financial institution that is involved in the correspondent account services.

Bearer Negotiable Instruments and Cash Payouts

- 5.15. Under the proposed FSM-N27 Notice, it was proposed for licensees to be prohibited from issuing bearer negotiable instruments. It was also proposed for licensees to be prohibited from paying cash out in an amount that is equal to or exceeds S\$20,000. Instead, if licensees are required to make



payments equal to or exceeding S\$20,000, it was proposed for them to use cheques, subject to certain conditions.

- 5.16. Respondents were generally supportive of the prohibitions. However, several respondents sought clarifications on the scope of the restrictions and expressed concerns about the operational constraints that may arise.

MAS' Response

- 5.17. Cash and bearer negotiable instruments are anonymous in nature and therefore susceptible to ML/TF risk. Hence, there is heightened ML/TF risk exposure inherent to such cash-based transactions. As such, MAS maintains our position on the proposed requirements and the prohibitions imposed on licensees issuing bearer negotiable instruments and restrictions on making cash payouts to mitigate the ML/TF risks.

Value Transfers

- 5.18. Under the proposed FSM-N27 Notice, it was proposed for licensees to adhere to value transfer requirements when effecting the sending of, receiving, or arranging for the value transfer of one or more digital tokens. These requirements include the type of information accompanying the transfer and the information to be retained which would vary depending on whether the licensee is the originating institution, beneficiary institution or intermediary institution.
- 5.19. Respondents generally agreed with the information required to accompany value transfers set out in the proposed Notice and that the information would also be relevant for law enforcement purposes. They have suggested that other useful information fields would include the transaction reference number and additional details relating to the digital token, such as type and amount. Some respondents have also suggested greater harmonisation of requirements with other jurisdictions, and the creation of uniform messaging standards.
- 5.20. Some respondents sought clarifications on the expectations on licensees in verifying the identity of the originator and beneficiary, including whether the value transfer can proceed if the required value transfer originator or beneficiary information is lacking.



MAS' Response

- 5.21. The information required to accompany value transfers as set out in the proposed Notice are aligned with the FATF standards. There is a variety of solutions that are available or being developed so to remain technology neutral, MAS does not intend to prescribe how Licensees should comply with the value transfer requirements in the Notice.
- 5.22. In relation to the verification of the identity of the originator and beneficiary, MAS would like to clarify that licensees, who are ordering institutions, are required to verify the value transfer originator's identity prior to effecting or arranging for the value transfer. If the licensee is a beneficiary or intermediary institution, it is required to take reasonable measures to identify value transfers that lack the required value transfer originator or beneficiary information and to implement risk-based policies, procedures and controls to determine when to execute, reject or suspend such value transfers and the appropriate follow-up action. For value transfers where the beneficiary institution pays out the transferred digital token(s) in cash or cash equivalent to the value transfer beneficiary, a beneficiary institution must identify and verify the identity of the value transfer beneficiary if the identity has not been previously verified. These requirements, amongst others, are set out in Paragraphs 14.3 to 14.20 of the proposed FSM-N27 Notice which contain the responsibilities of an ordering institution, an intermediary institution and a beneficiary institution.



6. Notices on reporting requirements, technology risk management and cyber hygiene

Reporting requirements

- 6.1. Under the proposed Notice on Reporting of Suspicious Activities and Incidents of Fraud (“FSM-N28 Notice”), it was proposed for licensees to lodge a report with MAS within the time specified in the notice upon the discovery of any suspicious activities or incidents of fraud if such activities or incidents are material to the safety, soundness or reputation of the licensee.
- 6.2. Several respondents requested for MAS to provide guidance on the criteria relating to suspicious activities or incidents of fraud. A respondent also sought clarification on whether an interim report could be submitted within the five-day reporting timeframe, followed by a final report after investigation is completed.
- 6.3. Under the proposed Notice on Submission of Regulatory Returns (“FSM-N29 Notice”), it was proposed for licensees to make periodic regulatory submission of information to MAS.
- 6.4. Respondents were generally agreeable with the proposed requirements for regulatory returns. However, some respondents proposed alternative reporting requirements, such as a decreased frequency of return submissions and the use of other factors in deriving the figures to be submitted, such as the use of an average monthly exchange rate instead of the exchange rate prevailing at the time of transaction.

MAS’ Response

- 6.5. In relation to the scope of reportable activities and incidents required under the FSM-N28 Notice, MAS does not intend to prescribe the materiality of a suspicious activity or incident of fraud. This would depend on various factors such as the amounts involved, the impact on the business operations, etc., which should be assessed by the licensee.



- 6.6. Regarding the proposed reporting timeline under the FSM-N28 Notice, licensees must submit a report on suspicious activities and incidents of fraud to the Authority within five working days upon the discovery of the activity or incident, if such activities or incidents are material to the safety, soundness or reputation of the licensee. If the licensee is still in the midst of investigation, the licensee should indicate the status of the investigation in the report and MAS may reach out to the licensee for more information.
- 6.7. The fields to be submitted under the FSM-N29 Notice were proposed to allow MAS to understand and monitor the profile of each licensee's DT services in order for MAS to conduct supervision on a more targeted basis. In this regard, a reduced frequency in return submissions or the use of other factors in deriving the fields to be submitted, such as average monthly exchange rate, may not provide MAS with adequate insight to tailor the supervision approach for each licensee. Hence, MAS will maintain our proposed requirements in the FSM-N29 Notice.

Technology risk management and cyber hygiene requirements

- 6.8. Under the proposed Notice on Technology Risk Management ("FSM-N30 Notice"), it is proposed for licensees to maintain a high level of reliability, availability and recoverability of critical IT systems and to implement IT controls to protect customer information from unauthorised access or disclosure.
- 6.9. Respondents were generally supportive of the requirements. Although respondents were agreeable on the need to report major incidents to MAS in a timely manner, several respondents raised concerns that it may be challenging for licensees to provide incident details to MAS within a short period of one hour, and proposed for a tiered reporting approach for relevant incidents (e.g., notify MAS within one hour upon discovery of a relevant incident and provide a subsequent update with more details within 24 hours).
- 6.10. Under the proposed Notice on Cyber Hygiene ("FSM-N31 Notice"), it is proposed for licensees to secure administrative accounts, apply security patching, establish baseline security standards, deploy network security devices, implement anti-malware measures and strengthen user authentication.
- 6.11. Respondents were generally supportive of applying the proposed cyber hygiene requirements to licensees. Some respondents proposed for MAS to review and include cyber hygiene practices



performed in other jurisdictions (for example, regular penetration testing, implementation of multi-factor authentication to all user accounts that have access to sensitive information).

MAS' Response

- 6.12. MAS would like to clarify that the objective of the one-hour notification requirement is to provide sufficient lead time for MAS to assess the wider impact of the incident on the industry and the public. After the initial notification, licensees may be requested to provide further updates on the reportable incident.
- 6.13. With regard to cyber hygiene requirements, MAS would like to clarify that the intent of the FSM-N31 Notice is to establish a set of fundamental cyber security measures that licensees must implement to protect against the most common cyber-attacks. This is in addition to the best practices in cyber security promulgated in the Guidelines on Risk Management Practices – Technology Risk (“TRM Guidelines”), which licensees are expected to adopt.
- 6.14. Nonetheless, we acknowledge the respondents’ comments to expand the scope of the FSM-N30 Notice and the FSM-N31 Notice and will carefully consider them as part of any future revisions.



7. Notices on Conduct and Disclosures and communications

- 7.1. The proposed Notice on Conduct (“FSM-N32 Notice”) sets out conduct requirements for licensees, such as the record of transactions, issuance of receipts, display of exchange rates and fees, and its operating days.
- 7.2. Respondents were generally supportive of the proposed conduct requirements. However, several respondents suggested for more flexibility in the requirement relating to minimum operation hours, such as varying the minimum operation hours based on the licensee’s size and nature of business, or allowing the operations of outsourced third parties, such as third party call centres, to count towards the requirement.
- 7.3. Under the proposed Notice on Disclosures and Communications (“FSM-N33 Notice”), it is proposed for licensees to provide customers with a specified risk warning statement to highlight to its customers, among other things, that they are exposed to the risk of being unable to recover all the money or DTs that they have paid to the licensee or any third parties under an arrangement by the licensee if the business of the licensee or the third party fails.
- 7.4. Respondents were generally supportive of the proposed requirements on disclosures and communications. However, several respondents proposed additional requirements such as (i) including risk warnings in multiple languages and (ii) establishing a standardised template for disclosures. A few also sought guidance on representations relating to the licensee’s scope of regulation by MAS, such as how it should be made and actions to be taken in the event of inaccurate disclosures.

MAS’ Response

- 7.5. On the proposed minimum operating hours set out in FSM-N32 Notice, MAS would like to clarify that the proposed minimum operation hours are to ensure that the public has ample opportunity to contact the licensee. This would include the licensee’s customers and other major stakeholders, such as supervisors and law enforcement agencies. Similar considerations would be applicable regardless of the size and nature of the DTSP’s business. Hence, MAS maintains our position to retain the proposed requirements for minimum operation hours.



- 7.6. In terms of disclosures under the FSM-N33 Notice, MAS would like to clarify that we have not set out requirements on the number and types of languages which licensees must provide the risk warning statement in, as this would be dependent on the business nature and customer base of each licensee. Due to the different types of nationalities of customers that each licensee may serve, licensees should establish internal processes to assess the necessity of providing the risk warning statements in multiple languages (and if necessary, the number and types of languages) to ensure that its customers are meaningfully warned of the relevant risks.
- 7.7. On representations in respect of the scope of a licensee's regulation by the MAS in any publicly available material, licensees must ensure that any representation it makes does not misrepresent the scope of the activities that it is licensed to carry out, as set out in paragraph 7(a)(i) of the FSM-N33 Notice. If licensees are made aware of inaccurate representations regarding their scope of regulation by MAS, they are expected to take reasonable steps to correct the inaccuracies as soon as practicable. Licensees should also establish internal processes to determine the impact of the inaccuracies on its customers to determine whether additional actions should be taken. For example, licensees may wish to inform customers of the inaccuracy. MAS does not intend to propose additional requirements in FSM-N33 Notice relating to inaccurate representations regarding the scope of a licensee's regulation by MAS at this juncture.



8. Guidelines applicable to licensees

- 8.1. MAS proposed for guidelines that apply to all financial institutions to also be applied to all licensees. This includes the Guidelines on Fit and Proper Criteria (“F&P Guidelines”), TRM Guidelines, Guidelines on Business Continuity Management and Guidelines on Outsourcing.
- 8.2. Respondents are generally supportive of the application of the aforementioned guidelines on licensees.
- 8.3. Several respondents suggested to expand the cybersecurity component within the TRM Guidelines to include specific risks associated with digital tokens.
- 8.4. One of the respondents requested for the F&P Guidelines to include sector-specific competencies and standardised self-assessment checklists which licensees can use in assessing the competence of relevant persons as defined in the F&P Guidelines.
- 8.5. Some respondents have also suggested to include case studies within the various guidelines which are specific to the DTSP industry.

MAS’ Response

- 8.6. MAS would like to clarify that the TRM Guidelines are principles-based and set out statements of industry best practices which financial institutions are expected to adopt. Licensees are required to apply the principles in the TRM Guidelines in their risk assessments over its business and establish effective processes and controls to manage the identified risks.
- 8.7. In relation to the F&P Guidelines, MAS would like to clarify that the F&P Guidelines provides a non-exhaustive list of factors which licensees should use in assessing the competence and capability of relevant persons (as defined in the F&P Guidelines). Specifically, in determining whether a relevant person is considered “competent and capable”, licensees are best placed to determine the necessary competencies that each role requires and are expected to set out its own assessment factors taking reference from the F&P Guidelines as set out above. Therefore, MAS will not be setting out additional criteria of “competence and capability” specific to the DTSP sector in the F&P Guidelines. However, MAS will consider engaging the DTSP sector to determine key concerns and establishing a set of FAQs to include criteria specific to the DTSP sector, if appropriate.



- 8.8. On the inclusion of sector-specific case studies in all other guidelines (e.g. Guidelines on Outsourcing), since the guidelines are applied to all relevant persons carrying out any activity regulated by MAS, we will similarly consider engaging the DTSP sector to determine key concerns and establishing a set of FAQs with case studies, if appropriate.



Annex A

List of respondents to the consultation paper on the Proposed Notice on Prevention of Money Laundering and Countering the Financing of Terrorism for Organised Market Operators Formed or Incorporated in Singapore

1. ACCESS (Singapore Cryptocurrency and Blockchain Industry Association), which requested for confidentiality of submission
2. Anduril Pte Ltd, which requested for confidentiality of submission
3. Baker McKenzie. Wong & Leow
4. Blockchain Association of Singapore
5. ChainArgos Pte Ltd, which requested for confidentiality over several responses in its submission
6. Circle Internet Singapore Pte Ltd
7. Company A, which requested for confidentiality of identity and several responses in its submission
8. Digital Treasures Center Pte Ltd, which requested for confidentiality of submission
9. Hedera Hashgraph LLC
10. Independent Risk Consultant
11. IOTA Foundation
12. IQEQ Regulatory Compliance Pte Ltd, which requested for confidentiality of submission



13. Notabene

14. Respondent A, who requested for confidentiality over several responses in his submission

15. Respondent B

16. Respondent C

17. Respondent D

Please refer to Annex B for the submissions.



Annex B

Submissions from respondents to the consultation paper on Proposed Regulatory Approach, Regulations and Notices for Digital Token Service Providers issued under the Financial Services and Markets Act 2022

Note: The table below only includes submissions for which respondents did not request confidentiality.

S/N	Respondent	Responses from respondent
1	Baker McKenzie. Wong & Leow	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>We are generally supportive of these proposals. That said, we have received feedback on the timeline for commencement of the licensing regime (see response to Question 4 below).</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>We refer to our general comments below in Question 4 in relation to individuals subject to the licensing requirements under this regime – in particular, that we assume that persons employed by overseas companies who respond to work emails while on vacation in Singapore should not be subject to licensing. If, however, such scenarios are subject to licensing, then we request that the Monetary Authority of Singapore ("MAS") consider lowering the quantum for individuals in the following context:</p> <p>(a) Where several individuals based in Singapore support an overseas licensed entity which carries on business outside of Singapore. For example, if the overseas licensed entity has three individuals based in Singapore, the individuals would have to pay a total of SGD 750,000 even though all three individuals may support the same overseas licensed entity.</p>



S/N	Respondent	Responses from respondent
		<p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>We are generally supportive of these proposals.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>We have the following general comments:</p> <p>1. Scope of Licensing Regime <u>Place of Business:</u> As the licensing provisions bring into scope individuals who, from a "place of business" in Singapore, carry on a business of providing digital token ("DT") services outside of Singapore, we would like to clarify whether the following scenarios would come within scope particularly given the broad definition of "place of business" as from "any location (including a kiosk that can be moved from one location to another) in Singapore used by the licensee for carrying on its business":</p> <p>(a) Given the prevalence of remote working arrangements, is it the policy intention to catch individuals employed by overseas entities but working from home or residential premises in Singapore? We assume that it is not the intention to catch persons who are employed by overseas companies responding to work emails while on vacation in Singapore however, we would like to request for some further guidance in relation to the following category of persons:</p> <p>i. Individuals providing DT services to overseas companies from their home in Singapore, perhaps on a consultancy basis.</p> <p>a. Permanent place of business: Further, if it is indeed the intention to capture such situations, would the individual's home address then be sufficient to satisfy the requirement for a "permanent place of business"?</p> <p>ii. Employees or directors of overseas companies on remote work arrangements which allow them to work from Singapore. In the case of such arrangements, it is not the intention to catch one-off, temporary, ad hoc arrangements but what are relevant factors to determine whether the arrangement is a permanent arrangement within scope?</p> <p>Based on the drafting of the current legislation, it is arguable that the above scenarios in (i) and (ii) should not be caught on the basis that home or residential premises are not commonly understood as a place through which a licensee would carry on business. However, if such individuals were to work from a co-working space or work from the offices of a related company of the overseas entity, then they would appear more clearly within scope as such premises are more easily</p>



S/N	Respondent	Responses from respondent
		<p>understood as a place from which a licensee would carry on business. In the case of individuals, the distinction between the two scenarios can be quite arbitrary so it would be helpful to clarify the policy intention here.</p> <p>2. Licensing of Individuals Subject to the above clarification on the scope of "individuals" caught by the licensing regime and noting that requirements under the proposed DT service provider ("DTSP") regime currently appear to apply equally to corporations, partnerships, limited liability partnerships and individuals holding a DTSP license, we query whether this parity in approach was intended, given the practical implications for individual licensees which may be disproportionately onerous for individuals with limited resources.</p> <p>Individual licensees would face logistical and practical difficulties meeting certain requirements - e.g. the permanent place of business requirements, the requirement to be present for prescribed hours, full AML/CFT policies and customer due diligence ("CDD") checks on all customers under the proposed FSM Notice N27 ("FSM AML Notice"). We would also like to clarify whether there will be exemptions from conduct of business requirements applicable for individuals. As such, we query whether the MAS can consider exemptions or adaptations for individual licensees. Please also refer to our further comments under Question 6.</p> <p>3. Transitional Arrangements and Commencement Timeline We note some concerns with the MAS' proposal not to have any transitional arrangement for DTSPs and that the period of four (4) weeks' notice may not be sufficient to make the relevant arrangements to prepare for the DTSP licensing regime. In particular, given that there will not be any grandfathering period and prospective DTSPs would need time to complete the license application process and receive confirmation that they have obtained the relevant license (the timeline for which is indeterminate at this point), before they can resume their current arrangements, we note requests that a period of three (3) months be provided before the commencement of the DTSP licensing regime. The view is that this period would allow for time to make the necessary arrangements so as to minimise impact on business operations and ensure that the customers' interests are not unduly prejudiced.</p> <p>We note that para 2.9(e) of the Consultation Paper (P010-2024) provides that "The applicant should have adequate compliance arrangements commensurate with the scale, nature, and complexity of their operations." The Consultation Paper provides an indication of the form such arrangements may take, namely: (i) an independent compliance function in Singapore; (ii) compliance support from holding company or overseas related entity; or (iii) appropriate compliance management arrangements (including at least, the appointment of a suitably qualified compliance officer based in Singapore, at the management level).</p>



S/N	Respondent	Responses from respondent
		<p>We read this to mean that it may be possible for DTSPs to outsource compliance to its overseas related entity without a dedicated compliance officer at management level in Singapore, depending on the scale, nature and complexity of its Singapore operations, among other listed alternate compliance arrangements.</p> <p>However Section 18.11 of FSM-N27 provides “A digital token service provider must develop appropriate compliance management arrangements, including at least, the appointment of an AML/CFT compliance officer, at the management level” which suggests that it is a requirement that all DTSPs must have an AML/CFT compliance officer at management level. This is inconsistent with the suggestion in para 2.9(e) of the Consultation Paper. Could MAS please clarify / confirm the language in Section 18 of FSM-N27 will be amended?</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>We are generally supportive of these proposals.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>We note that one of the MAS' criteria for DTSP applicants is that they are already regulated and supervised for compliance with relevant internationally agreed standards. For DTSP applicants that are already licensed overseas as payment service providers and subject to AML/CFT requirements that are in line with FATF standards, we note that under the AML Notice proposed under this regime, they will not be able to rely on the CDD measures carried out by their overseas entities if such overseas entities are payment services providers. We note that this is consistent with the approach taken under PSN02.</p> <p>However, we query whether this is necessary in the context of this DTSP regime, recognising that there could be some differences in the AML/CFT requirements in the overseas jurisdictions with those required under the FSM AML Notice and particularly since DTSPs would not have Singapore customers or business in Singapore. Many DTSP applicants are likely to rely on existing compliance officers of their overseas regulated entities who are already responsible to ensure AML/CFT and CDD compliance with the requirements of their home regulator. We query whether it is efficient to require these compliance officers to repeat CDD, albeit for compliance with the FSM AML Notice, particularly when there will not be any new customers since there is no business in Singapore. The concern here is that this creates an extensive tick-the-box exercise for overstretched teams that then distracts from sufficient attention being paid to detect and address real AML/CFT risks or threats.</p>



S/N	Respondent	Responses from respondent
		<p>Further, as drafted, the FSM AML Notice will need to be complied with equally by individual DTSPs and there may be practical issues with individual DTSPs ensuring full compliance with all aspects of the FSM AML Notice, particular in respect to CDD checks, screening and transaction monitoring checks.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>We are generally supportive of these proposals.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>No comments.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>We are generally supportive of these proposals.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>No comments.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>No comments.</p>



S/N	Respondent	Responses from respondent
		<p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>We note concerns that where the DTSP (or its foreign branch), given its overseas customer base, is already subject to such requirements under another regulatory regime, this would result in multiple layers of similar requirements and necessitate a gap analysis between the different regimes. We request that MAS considers allowing for exemptions where a DTSP is already regulated in a foreign jurisdiction on the basis that it is carrying on business and servicing customers in such foreign jurisdiction and not in Singapore. Recognising that there may be different standards depending on the licensing regime in the foreign jurisdiction, we query whether MAS can consider setting out a whitelist of certain jurisdictions where, assuming the DTSP holds certain licenses in such jurisdictions, they could benefit from exemptions from certain requirements applied to DTSPs.</p> <p>Further, we query whether the cyber hygiene requirements are necessary considering that no customer in Singapore is affected by the business operations of DTSPs and whether the MAS can consider exemptions for DTSPs already licensed or regulated overseas.</p> <p><u>Critical Systems</u> Given the typical business model of a DTSP and its overseas-based customer base, it is anticipated that "critical systems" will usually be located overseas. Further, we would like to seek clarity on the meaning of "critical system" to an individual DTSP, given that the scale of an individual's operations will likely be significantly smaller than that of a corporation etc. We request that MAS consider exemptions for DTSPs already licensed or regulated overseas.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>We query whether the requirement for presence at the DTSP's permanent place of business for at least 10 days a month, for at least eight hours on each of those days, is necessary given that the DTSP's customers will be located outside Singapore. We note that the justification provided by MAS for this requirement is "to ensure that the public has ample opportunity to reach the licensee", but query if this may be of limited relevance given the reality of a DTSP's business operations, where its customers are outside of Singapore.</p> <p>Further, we request that MAS consider if flexibility and/or exemptions should be available for individual DTSPs.</p>



S/N	Respondent	Responses from respondent
		<p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>We note that administrative difficulties may arise in respect to the implementation by DTSPs of certain MAS Guidelines, most notably the Guidelines on Outsourcing.</p> <p>For example, established DTSPs with operations or customers outside Singapore will likely have various pre-existing engagements with third party service providers overseas, which may be affected by the requirements in the Guidelines on Outsourcing. We therefore propose that: (a) if the DTSP (or its foreign branch) is already regulated in overseas jurisdictions, these DTSPs should be exempt from complying with the Guidelines on Outsourcing, otherwise a double layer of regulatory requirements (which may have contradictory expectations) will be imposed on such arrangements; and/or (b) in any case, the Guidelines on Outsourcing should not apply to existing outsourcing agreements or the DTSPs should have a grace period for complying with the Guidelines on Outsourcing.</p> <p>Further, we consider that an individual DTSP would face particular difficulties in complying with these requirements, and wish to clarify if a graduated approach should apply to individuals (as opposed to be DTSPs that are entities).</p>
2	Blockchain Association of Singapore	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>The Regulatory and Compliance Sub-Committee of BAS is pleased to set out BAS’s comments on the Consultation Paper. We had conducted a members’ seminar on 30 October 2024, which was attended by 32 persons. These responses consider comments received at the seminar.</p> <p>Capitalised terms used in the responses below (that are not defined) have the same meaning as that set out in the Consultation Paper.</p> <p><u>General comments</u> Scope of the FSM Act – factors in assessing whether a Singapore entity has limited nexus to Singapore</p> <p>We note that the MAS generally expects to grant a DTSP licence in extremely limited circumstances, as:</p> <ul style="list-style-type: none"> (a) in most cases, persons that are operating from a place of business in Singapore or incorporated or formed in Singapore, will carry on a business of providing DT services in Singapore; and (b) as such, they would typically be subject to the MAS’ regulatory oversight under other regulatory regimes (e.g. the PS Act).



S/N	Respondent	Responses from respondent
		<p>Notwithstanding that Part 9 of the FSM Act is intended to align with the FATF standards, we note that this new regulatory regime has not yet been adopted by a number of major jurisdictions. Hong Kong regulations for example, are still currently focused on controlling activities in Hong Kong (as opposed to Part 9 of the FSM Act, which looks towards DT services provided outside Singapore). As such, there is relatively little clarity on how this FATF standard is intended to apply in practice / on a global scale, in order to mitigate regulatory arbitrage risks.</p> <p>Based on our observations, key scenarios where a Singapore entity would have a limited nexus to Singapore would include:</p> <ul style="list-style-type: none"> (a) where the Singapore entity only serves to house its senior management and directors; and/or (b) where the Singapore entity is being set up solely for purposes of establishing a Singapore tax residency, and all other activities / operations of the Singapore entity are located outside Singapore. <p>We would be grateful if the MAS could clarify / provide further guidance on whether the above scenarios are in line with its regulatory approach on entities that will be caught under Part 9 of the FSM Act, and if it has other factors in mind.</p> <p>Scope of the FSM Act – AML/CFT obligations and oversight</p> <p>As mentioned above, we note that Part 9 of the FSM Act is intended to align with the FATF standards, with the FATF’s primary concern being differences in AML/CFT obligations and oversight between the jurisdiction where the DTSP is incorporated/created, and the jurisdiction where the products and services are offered.</p> <p>However, we note that the regulatory requirements imposed on DTSPs include financial requirements, business conduct, technology risk management, cyber hygiene, and audit requirements.</p> <p>We would be grateful if the MAS could clarify its intent behind expanding the regulatory requirements beyond AML/CFT concerns.</p> <p>Scope of the FSM Act – licensing perimeter</p> <p>On a related note, due to the different licensing perimeter of the FSM Act, the PS Act, the SFA and the FAA, there arises a situation where an entity who provides advice in relation to digital payment tokens (e.g. by issuing research reports):</p> <ul style="list-style-type: none"> (a) is presently not caught under the FAA, SFA and/or the PS Act (as digital payment tokens are not “investment products” or “capital markets products”); and (b) may be caught under the licensing perimeter of the FSM Act, specifically limb (j) of the prescribed DT services in Part 1 of the First Schedule to the FSM Act (“Limb J”).



S/N	Respondent	Responses from respondent
		<p>We would be grateful if the MAS could clarify the below:</p> <p>(a) Whether it is the MAS’ policy intention to regulate such entities (as described in the scenario above) under the FSM Act?</p> <p>To explain:</p> <p>(i) such entities would technically not be exempted from licensing under the FAA, SFA and the PS Act (as such activities are not licensable to begin with); and</p> <p>(ii) as such, these entities would not be able to rely on the carve out under section 137(5) of the FSM Act.</p> <p>(b) In connection with (a) above, if the MAS’ policy position is that such entities would be caught under Part 9 of the FSM Act, could the MAS kindly further clarify which aspects of the entity’s business will become regulated under the FSM Act (i.e. only the DT services that are provided outside Singapore, or the entire business line including DT services provided in Singapore)?</p> <p>(c) Whether Limb J is intentionally worded more broadly than a “financial advisory service” under the FAA?</p> <p>To elaborate:</p> <p>(i) Limb J includes any service relating to the sale or offer of digital tokens which involves (1) providing advice, either directly or through publications or writings, and whether in electronic, print or other form, relating to any digital tokens, or (2) providing advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, relating to any digital tokens; and</p> <p>(ii) the definition of a “financial advisory service” under the FAA does not include the wording "relating to the sale or offer of" (in respect of investment products).</p> <p>If Limb J is intentionally worded more broadly, could the MAS clarify how participants should distinguish research reports that relate to the sale or offer of digital tokens (for example, would traditional research reports that are generic in nature be caught, or is something else needed)?</p> <p>Enforcement and consumer protection measures against unlicensed entities</p> <p>We understand that Part 9 of the FSM Act is intended to ensure a level playing field among virtual asset service providers (“VASPs”). In this spirit, while we note that there is a prohibition against solicitation by unlicensed entities under section 9 of the PS Act, we wanted to clarify / better understand:</p>



S/N	Respondent	Responses from respondent
		<p>(a) the MAS’ enforcement strategy and focus on unlicensed entities that solicit Singapore customers; and</p> <p>(b) whether the MAS intends to introduce further safeguards under existing regulations.</p> <p>For context:</p> <p>(a) in relation to (a) above, we understand that in the UK, in addition to a prohibition against soliciting crypto related services to the UK public (similar to the section 9 prohibition under the PS Act), recently released data (https://www.fca.org.uk/data/financial-promotions-quarterly-data-2024-q3) shows that the UK Financial Conduct Authority has issued 1,702 consumer alerts about illegal crypto promotions, and enforcement action resulted in the take down of over 900 scam crypto websites and the removal of 56 apps from UK app stores; and</p> <p>(b) in relation to (b) above, we understand that in South Korea, among other measures, their travel rule requirements prohibit dealings with unregulated / unregistered foreign VASPs that target Korean customers. Practically, this limits the scale of operations / activities that unlicensed VASPs can conduct. In Hong Kong, the Securities and Futures Commission (“SFC”) also maintains a complaint form (https://www.sfc.hk/en/Lodge-a-complaint/Against-intermediaries-and-market-activities/Online-Complaint-Form), which can be used to alert the SFC of unlicensed entities. The alert list on the SFC website (https://www.sfc.hk/en/Alert_List) also suggests that the SFC has been rather active in its enforcement focus on VASPs.</p> <p>We would be grateful if the MAS could give the industry an update on whether similar measures are contemplated.</p> <p>Timeline for licence application</p> <p>We have received feedback that the four weeks’ notice prior to the commencement of the DTSP Provisions (as defined in the Consultation Paper) would unlikely be sufficient for affected persons to apply for a DTSP licence.</p> <p>Participants have flagged that the prescribed Form 1 (for purposes of submitting a DTSP licence application), and accompanying documents that has to be submitted with Form 1, is not yet made available. For example, where the DTSP licence application has to be accompanied by:</p> <p>(a) the applicant’s policies and procedures (such as AML/CFT policies as is the case for a licence application made under the PS Act);</p> <p>(b) attestation / assurance reports conducted by an external auditor; and/or</p> <p>(c) a legal opinion on why the applicant is caught under the FSM Act (and not the PS Act, SFA or FAA), such information / documents would require substantive time to be put together.</p>



S/N	Respondent	Responses from respondent
		<p>As there is uncertainty as to the volume and type of information applicants would need to put together to make a DTSP licence application, we would be grateful if the MAS could consider:</p> <ul style="list-style-type: none">(a) releasing the prescribed Form 1, together with accompanying documents / information needed (including standards that the MAS expects of these documents) ahead of finalising the DTSP Provisions; and/or(b) providing a longer notice period (e.g. 2 – 3 months) prior to the commencement of the DTSP Provisions. <p>Separately, given that affected persons who are conducting DT activities outside Singapore would be required to suspend or cease operations once the DTSP Provisions come into force, until they are granted a DTSP licence (or are appropriately exempted), we would be grateful if the MAS could provide some guidance on how long it expects to take, when processing DTSP licence applications.</p> <p>Timeline for lapsing of DTSP licence, fee structures and quantum of fees</p> <p>We have no comments to the timeline for the lapsing of a DTSP licence, as well as the licence application and annual fees proposed.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>Subject to our general comment above (on AML/CFT obligations and oversight), we have no further comments to the minimum initial and ongoing financial requirements proposed in the Consultation Paper.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>We have no comments to these provisions under the proposed FSM Regulations.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>Subject to our general comment above (on AML/CFT obligations and oversight), we have no further comments to Parts 6 – 8 of the Consultation Paper.</p> <p>Our comments for Part 5 of the Consultation Paper are set out in the specific questions below.</p>



S/N	Respondent	Responses from respondent
		<p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>We have no comments to the requirement for DTSP licence holders to perform CDD measures as required under the proposed Notice FSM – N27 on existing customers (i.e. customers of the DTSP licence holders prior to them obtaining their DTSP licence).</p> <p>However, we would be grateful if the MAS could clarify if:</p> <ul style="list-style-type: none">(a) it intends to prescribe a maximum time period for such CDD measures to be completed; and(b) if so, to consider providing a sufficient time period (e.g. 3 – 4 months), taking into consideration that various DTSPs have different scale of operations, and some players may be required to conduct CDD on a large volume of existing customers. <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>We have no comments on the requirements for DTSP licensees to rely on a third party to perform CDD measures – we note that these requirements are aligned with the AML/CFT notices for other classes of financial institutions (e.g. PS Act licence holders).</p> <p>On the MAS’ intention to continue precluding financial institutions from relying on third parties that are licensed payment service providers, DTSP licence holders, or persons who hold equivalent licences, we would be grateful if the MAS could continue to monitor the level and standard of AML/CFT controls across the payments sector, and keep an open mind to removing this exclusion in the future, when the payments sector’s AML/CFT controls are of an equivalent standard to other classes of financial institutions in the financial services industry.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>Please see our response to question 6 above.</p>



S/N	Respondent	Responses from respondent
		<p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>We have no comments to paragraph 12 of the proposed Notice FSM – N27. We note that these requirements are aligned with the AML/CFT notices for other classes of financial institutions (e.g. PS Act licence holders).</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>We have no objections to paragraph 10 of the proposed Notice FSM – N27. We note that these requirements are aligned with the AML/CFT notices for other classes of financial institutions (e.g. PS Act licence holders).</p> <p>We would comment however, that allowing DTSP licence holders (and other classes of financial institutions) to use cheques to make payment of S\$20,000 and above, may soon become obsolete, given the MAS’ intention to eliminate corporate cheques by 2025.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>We have no comments to paragraph 14 of the proposed Notice FSM – N27.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>We have no comments to the proposed Notice FSM – N28 and FSM – N29.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>Subject to our general comment above (on AML/CFT obligation and oversight), we have no further comments to the proposed Notice FSM – N30 and FSM – N31.</p>



S/N	Respondent	Responses from respondent
		<p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>We have no comments to the proposed Notice FSM – N32 and FSM – N33.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>We have no comments to the application of these guidelines to DTSP licence holders.</p>
3	ChainArgos Pte Ltd	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>No comment.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>No comment.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>No comment.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>No comment.</p>



S/N	Respondent	Responses from respondent
		<p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>No comment.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Prohibiting reliance on entities with only PS Act, or similar, licenses is appropriate. Further, it remains appropriate to permit reliance on entities with licenses akin to a Banking License or Capital Markets Services License. In general companies which in the ordinary course of their business are providing or holding themselves out to be providing payment services should also be precluded from relying on third party licensees that only hold a PS Act, or similar, license.</p> <p>There are many examples of licensed payment services providers in other jurisdictions not being held to the same AML/KYC/CFT or sanctions screening standards expected of banks and other more-stringently-regulated financial institutions, despite processing significant transaction volumes.</p> <p>Such regulatory gaps have often been exploited by payment processing companies under the guise of “fintech” with Wirecard being one infamous example, and more recently, Payrnet, a UK-regulated electronic money institution (EMI) that lost its EMI license in Lithuania, because of a lack of clarity regarding its ultimate beneficial owners, but was somehow still able to continue operating under its separately-supervised UK EMI license .</p> <p>Neither are these issues specific to any one region either, as evidenced by the US experience of Synapse, Evolve Bank and other “banking as a service” providers.</p> <p>Behind the veneer of “technology” many payment service providers facilitate significant transaction volumes, without the same levels of compliance and oversight present in wholesale financial services.</p> <p>This is not to say any fault lies with the regulatory authority, but rather to highlight the risks present when the payment service providers are held to a lower standard of compliance and oversight than banks and other financial institutions.</p> <p>Harmonizing compliance standards for both financial institutions and payment service providers is the best way to combat the global rise in money laundering, terrorism financing, and sanctions evasion, to plug gaps in overseeing transfers of value. Preventing SG-licensed entities from relying on foreign-licensed institutions</p>



S/N	Respondent	Responses from respondent
		<p>with only money-transmitter-type licenses would be a useful step towards those larger goals.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>No comment.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>For correspondent account services, the licensee is relying on their client’s standard of compliance in a manner similar to the “Reliance on Third Party” issues discussed in previous questions.</p> <p>It would therefore be preferable to harmonize such compliance requirements, to prevent regulatory gaps between service providers from being exploited, especially given the economic activity, the facilitation of payments, remains fundamentally the same.</p> <p>While, such harmonization is a larger, long-term goal, against the backdrop of fostering innovation without necessarily facilitating illicit fund flows, applying the FATF correspondent banking framework is a good first step.</p> <p>Applying the FATF correspondent banking framework to payment service providers, especially where intermediary relationships resemble those of a correspondent bank, should be the preferred approach.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>It is unclear if the intention is to exclude stablecoins from this prohibition, and if so, such exclusion should be made explicit.</p> <p>The relevant portion of the current definition of bearer negotiable instrument reads “any negotiable instrument that is in bearer form, indorsed without any restriction, made out to a fictitious payee or otherwise in such form that title thereto passes upon delivery.”</p>



S/N	Respondent	Responses from respondent
		<p>Before the development of stablecoins, digital tokens intended to be used as the functional equivalent of currency, such a definition was clear.</p> <p>However, the current definition could be further strengthened by clarifying whether the definition of “bearer negotiable instruments” ought to be extended to stablecoins.</p> <p>A 2023 BIS report on stablecoins suggests, “in one model, which resembles current asset-backed stablecoins, private tokenized money circulates as a digital bearer instrument.”</p> <p>There are also plenty of blockchain projects, teams, and organizations which hold out their token offerings as some form of bearer instrument, and as such, clarity in the definition of “bearer instrument” would better guide compliance practices.</p> <p>Unless the intention is to prevent licensees from transacting in stablecoins – this does not appear to be the case and we are not recommending it – clarifying the definition would be helpful in preventing confusion in discussions with overseas counterparties.</p> <p>Exacerbating the challenge with stablecoins is that they exist in several varieties, and as technology evolves, the manner in which stablecoins are issued will continue to change.</p> <p>For instance, there are currently stablecoins with centralized issuers, and those which purport to be “decentralized” and it would not be ideal that characterizing a stablecoin as “decentralized” should somehow exempt it from regulatory oversight.</p> <p>If the ill effects of the illicit flow of funds is the public harm that is sought to be avoided, but the ease and speed of fund transfers is the economic good that is desired, then clarity in such definitions, and the construction of a framework for effective monitoring and oversight would be preferred.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>No comment.</p>



S/N	Respondent	Responses from respondent
		<p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>No comment.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>No comment.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>No comment.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>No comment.</p>
4	Circle Internet Singapore Pte Ltd	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>NA - proposed regulatory framework does not apply to Circle SG. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>NA - proposed regulatory framework does not apply to Circle SG. Explanatory note submitted to Case Officer dated 28/10/2024.</p>



S/N	Respondent	Responses from respondent
		<p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>NA - proposed regulatory framework does not apply to Circle SG. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p>



S/N	Respondent	Responses from respondent
		<p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p>



S/N	Respondent	Responses from respondent
		<p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>NA - proposed regulatory framework does not apply to Circle Singapore. Explanatory note submitted to Case Officer dated 28/10/2024.</p>
5	Company A	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>We do not have further comments.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>We do not have further comments.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>[Confidential].</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>[Confidential].</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>[Confidential].</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>We do not have further comments.</p>



S/N	Respondent	Responses from respondent
		<p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>[Confidential].</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>We do not have further comments.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>We do not have further comments.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>We do not have further comments.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>We do not have further comments.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>We do not have further comments.</p>



S/N	Respondent	Responses from respondent
		<p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>We do not have further comments.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>We do not have further comments.</p>
6	Hedera Hashgraph LLC	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>Overall, the proposed regulations aim to create a stable and regulated environment for digital token service providers (DTSPs) to protect consumers and investors, prioritizing financial security and transparency. However, the relatively high costs and strict conditions may limit entry to more established companies, potentially hindering innovation by smaller ventures or start-ups.</p> <p>The requirement to lodge specific forms and comply with detailed regulations could create an administrative burden for new ventures or startups that might lack dedicated compliance teams. While the lapsing criteria ensures active participation, it might be too stringent, particularly for startups that need time to build their services or those facing temporary operational setbacks might risk losing their license, which can hinder their ability to grow.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>The minimum base capital or security requirement of \$250,000 may act as a barrier to entry for smaller companies and startups. We recommend that these financial requirements be levied on a progressive basis.</p>



S/N	Respondent	Responses from respondent
		<p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>Given the nature of digital token services, cybersecurity threats and risks are a major concern. Ensuring that top leadership is directly responsible for implementing and monitoring risk management protocols can enhance the security of the platform and protect users. Specifying that the CEO and directors must establish and maintain a comprehensive cybersecurity policy to safeguard digital assets provides clarity over allocation of responsibilities. Additionally, they should be responsible for overseeing risk management strategies, including contingency planning.</p> <p>The digital token industry is fast-evolving, and staying updated with the latest regulations, technologies, and risks is essential for effective governance and risk mitigation. The audit requirements in Annex C aim to promote accountability, transparency, and compliance across the digital token service industry. While this helps in fostering trust and stability, the increased costs, administrative burden, and strict timelines may disproportionately affect smaller companies and individual operators. Balancing these stringent requirements with potential exemptions or scaled-down requirements for smaller entities might address some of these concerns.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>Nothing to add for parts 5-8.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>Nothing to add regarding the requirements for existing customers.</p> <p>However, we recommend that companies operating in the Layer 2 space should be subject to the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Third-party reliance on AML/CTF controls can be appropriate for DTSPs, particularly for smaller firms looking to leverage specialized expertise and technology. Relying</p>



S/N	Respondent	Responses from respondent
		<p>on third-parties can be very beneficial for smaller DTSPs. Some advantages can include scalability, cost and resource efficiency. For smaller DTSPs, third-party reliance can enhance the robustness of their CDD procedures, particularly if the third-party has a strong track record and is compliant with industry standards and best practices. However, we note that relying on third-parties for customer due diligence (CDD) exposes DTSPs to a number of risks.</p> <p>Some of these risks include reduced control and oversight, data security/privacy concerns and dependency risk.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>Nothing to add with regard to amendments to the other AML/CFT notices.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>The provision of Correspondent Account Service involves significant regulatory compliance burdens. Licensees must adhere to stringent Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) requirements, including thorough customer due diligence (CDD), risk assessments, and ongoing monitoring of financial partners. This necessitates assessing the suitability of other financial institutions, understanding and documenting AML/CFT roles, and obtaining senior management approval for new relationships. For small ventures and start-ups in the digital asset and blockchain industry, offering or engaging in Correspondent Account Services can present several challenges. Small businesses often lack the financial resources and dedicated compliance teams that larger firms have, making it difficult to implement thorough risk assessments, ongoing monitoring, and customer due diligence. This can lead to increased operational expenses, diverting resources from core business activities and potentially stifling growth.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>Prohibiting cash payouts above a certain threshold and requiring the use of cheques, or other payment methods, may slow transaction settlement, add administrative burdens, and limit the ease of conducting business potentially incur additional costs.</p>



S/N	Respondent	Responses from respondent
		<p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>In the context of MAS Notice FSM-N28, which addresses suspicious activity reporting and risk management, it's essential to consider the differences between Layer 1 and Layer 2 on blockchain networks. Layer 1 (e.g., Hedera Hashgraph) serves as the infrastructure backbone, enabling interoperability and data transfer between various blockchains. Layer 1 networks are primary blockchains where transactions and messages are directly validated and recorded on the main ledger. Layer 2 solutions, including tokenization products and financial tools, are built on top of Layer 1.</p> <p>We recommend that companies operating in the Layer 2 space should be responsible for collecting, maintaining and processing this information as they have the interface with customers.</p> <p>There are several industry-wide initiatives and blockchain associations, designed to support compliance with the value transfer requirements, that also aim to streamline processes, reduce compliance burdens, and promote standardized practices, across the digital asset and blockchain sector, especially beneficial for small ventures and start-ups. These include travel rule protocols, interVASP messaging standards, blockchain monitoring tools, and global associations like GDF, ISO and ICC:</p> <p>Travel Rule Protocols and Solutions: Travel Rule Information Sharing Alliance (TRISA), Travel Rule Universal Solution Technology (TRUST) and VerifyVASP are collaborative industry initiatives that help digital asset service providers (VASPs) comply with the Financial Action Task Force (FATF) "Travel Rule," similar to MAS and FATF requirements. These protocols enable the secure exchange of originator and beneficiary information between VASPs, reducing the complexity of compliance and improving data accuracy. Solution interoperability between TRISA, TRUST and other TR Service Providers would be beneficial for the industry.</p> <p>InterVASP Messaging Standards (IVMS 101): Though not a global standards board, IVMS 101 was developed by a coalition of industry groups, including GDF, the Chamber of Digital Commerce, and IDAXA (International Digital Asset Exchange Association). It is a technical standard that ensures consistent data sharing for compliance with the FATF Travel Rule. By creating a unified message format, it simplifies how VASPs handle originator and beneficiary information efficiently.</p>



S/N	Respondent	Responses from respondent
		<p>Blockchain Analytics and Monitoring Tools: Chainalysis, Elliptic, and TRM Labs offer advanced blockchain analytics tools that assist with transaction monitoring and compliance. These solutions can help businesses automatically flag suspicious transactions, conduct enhanced due diligence (EDD), and generate the necessary reports to meet regulatory standards. By outsourcing part of the compliance process to specialized providers, small ventures can reduce the need for in-house expertise.</p> <p>Global Digital Finance (GDF): GDF is a leading global association that develops best practices and frameworks for the digital asset sector. It brings together regulators, industry participants, and stakeholders to establish guidelines that ensure compliance with global AML/CFT standards, including the Travel Rule. GDF's Code of Conduct outlines practices that help businesses navigate complex compliance requirements while fostering innovation and growth in the digital asset ecosystem.</p> <p>International Organization for Standardization (ISO): ISO develops global standards for a wide range of industries, including digital assets and blockchain. Standards like ISO/TC 307 focus on blockchain and distributed ledger technologies, addressing issues such as security, interoperability, and compliance. By promoting uniform standards, ISO helps ensure that businesses across different countries can follow consistent practices.</p> <p>International Chamber of Commerce (ICC): The ICC engages in promoting international trade and commerce standards, including for digital assets and blockchain technology. It collaborates with industry participants and regulators to establish standards that improve transparency, facilitate trade finance, and ensure compliance. While not specifically focused on value transfers, the ICC's work on digital trade guidelines helps to address broader compliance challenges in cross-border digital, or value transfer, transactions.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>By incorporating suggested improvements below, the MAS Notice FSM-N28 could align more closely with industry best practices and offer clearer, more robust guidelines for licensees, ensuring better compliance and more efficient handling of suspicious activities and fraud incidents.</p> <ol style="list-style-type: none"> 1. Enhance definitions with clarifications of what constitutes suspicious activities or incidents of fraud, including specific examples. Clarify and expand the definitions in the MAS Notice to include various types of suspicious activities, potentially with examples for easier identification by licensees. 2. Specific reporting channels or mechanisms (e.g., online portals, secure APIs) to streamline the submission of reports. The MAS Notice could introduce more modern and secure channels (such as dedicated digital platforms) for reporting, ensuring faster and safer communication.



S/N	Respondent	Responses from respondent
		<p>3. Detailed reporting templates and requirements for reporting, ensuring that all relevant information is captured. Expand the requirements in Form F1 of the MAS Notice to include additional fields that capture details on the nature of the suspicious activity, digital traces, and internal controls that failed or succeeded, helping authorities assess and act more effectively.</p> <p>4. Require the integration of a risk assessment framework to identify potential fraud before it occurs. Encourage licensees to implement or integrate risk assessment tools and methodologies to detect potential fraudulent activities proactively.</p> <p>5. Timely reporting and urgency protocols for different types of incidents, including faster timelines for high-risk activities. Introduce more nuanced timelines in the MAS Notice for reporting based on the severity and potential impact of the incident. For example, critical incidents could have a shorter reporting window than less severe ones.</p> <p>6. Clearer coordination with Law Enforcement (LE), especially for large-scale or sophisticated fraud cases. The MAS Notice could benefit from more detailed guidelines on how licensees should coordinate with law enforcement and any additional authorities when handling large-scale or complex cases.</p> <p>By incorporating suggested improvements below, MAS Notice FSM-N29 could enhance the regulatory returns submission process, aligning it more closely with modern compliance standards and fostering a more robust and transparent digital token ecosystem.</p> <p>1. Digital submission and automation through APIs, reducing manual errors and streamlining the process. Implement digital platforms that support automated submissions and real-time data synchronization, allowing licensees to submit regulatory returns via secure APIs directly from their internal systems.</p> <p>2. Enhanced data standardization to ensure consistency and comparability across different submissions. Enforce stricter data standardization, requiring licensees to submit returns using predefined data formats to facilitate easier analysis and integration for regulatory purposes.</p> <p>3. Incorporation of risk-based reporting framework to allow DTSPs to prioritize submissions based on assessed risk levels. Introduce risk-based reporting requirements under which higher-risk transactions or activities must be reported more frequently or in greater detail, helping to focus regulatory oversight on areas with greater risk exposure."</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>By incorporating suggested improvements below, the MAS Notice FSM-N30 could establish more robust, proactive, and comprehensive technology risk management practices, aligning closely with advanced regulatory frameworks worldwide.</p>



S/N	Respondent	Responses from respondent
		<ol style="list-style-type: none"> 1. Enhanced Incident Response and reporting protocol with clear steps for different types of incidents and designated points of contact for immediate actions. Expand the MAS Notice to include a structured incident response plan detailing roles, responsibilities, and escalation paths. Specify immediate actions to be taken upon discovery of different types of incidents (e.g., DDoS attacks vs. data breaches) and establish designated contact points for streamlined communication. 2. Broader coverage of critical systems or examples of what constitutes a critical system, emphasizing a broader range of components such as cloud services, backup systems, and middleware. The MAS Notice can enhance clarity by including examples of critical systems, ensuring that providers consider a wider range of potential vulnerabilities, including those related to cloud services, APIs, and third-party software dependencies. 3. Strengthened Data Protection measures requiring more robust encryption standards, multi-factor authentication, and frequent audits of access controls to safeguard sensitive customer data. Enhancing IT controls by specifying requirements for encryption (both at rest and in transit), multi-factor authentication for access to critical systems, and regular audits of user access helps ensure adherence to best practices in data protection. 4. Inclusion of a continuous monitoring framework to detect anomalies and potential threats in real time, rather than periodic checks. Include requirements for continuous monitoring and real-time alerting systems that detect anomalies or suspicious activities, facilitating proactive threat detection and faster incident response. 5. Comprehensive Disaster Recovery and Business Continuity Planning with specific scenarios and testing requirements. Expand on the existing RTO (Recovery Time Objective) guidelines by requiring comprehensive DR and BCP strategies. Include scenarios for different types of disruptions (e.g., cyber-attacks, hardware failures, natural disasters) and specify regular testing and drills to validate the effectiveness of these plans. <p>By incorporating suggested improvements below, the MAS Notice FSM-N31 would align more closely with best practices in cyber hygiene seen in other jurisdictions, fostering a stronger and more adaptive cybersecurity posture within Singapore's digital asset ecosystem.</p> <ol style="list-style-type: none"> 1. Risk-Based Approach where entities must align their security measures with the severity of risks they face. MAS Notice could further elaborate on a risk assessment framework, guiding service providers on prioritizing security measures based on risk levels (e.g., timeframes for patching critical vs. non-critical systems). 2. Data Protection and Encryption Standards (both at rest and in transit), as well as requirements around data backup and recovery. Enhancing the MAS Notice by setting clear data encryption requirements could help reinforce the protection of customer information. It could also mandate regular data integrity checks and secure backup practices.



S/N	Respondent	Responses from respondent
		<p>3. Third-Party Risk Management to enforce strict standards for managing third-party risks, including contractual requirements and ongoing monitoring. MAS could expand the scope of cyber hygiene to include more explicit guidance on how digital token service providers should vet, onboard, and continuously assess third-party vendors' security practices.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>Based on the MAS Notice FSM-N32 on Conduct for for DTSPs, here are some potential recommendations for improvements regarding operating days and hours:</p> <ol style="list-style-type: none"> 1. The requirement for a licensee to have at least one person present for a minimum of 10 days a month and at least 8 hours each of those days could be made more flexible. For smaller operators or those primarily providing services online, eliminating mandatory physical days could be considered, provided there are clear digital support alternatives (e.g., AI CSR bots, helplines, online chat channels, etc). 2. The current notice requires written advance notification for planned non-operating days. Instead, licensees could be permitted to use automated systems that instantly notify customers of any unplanned changes in real-time, especially during service disruptions, rather than relying on traditional written communication alone. <p>Based on the MAS Notice FSM-N33 on Disclosures and Communications for DTSPs, a potential recommendation for improvement regarding disclosure requirements would be to ensure consistency across the industry, MAS could introduce standardized templates for risk warnings and disclosures. This would make it easier for customers to compare services between providers and understand their exposure to risks without confusion.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>While adherence to MAS's risk guidelines provides numerous benefits for Digital Token Service Providers (DTSPs), there are also some potential challenges including (1) increased operational costs due to compliance and technology investments, (2) complexity and resource allocation administration, time and effort, (3) barriers to innovation slowing product development and inelastic process, and (4) vendor management challenges due to complex arrangements and risk of vendor non-compliance.</p>



S/N	Respondent	Responses from respondent
		<ol style="list-style-type: none"> 1. Increased operational costs due to compliance and technology investments. Adhering to stringent risk management, business continuity, and outsourcing guidelines can be costly. DTSPs may need to invest significantly in security infrastructure, backup systems, staff training, and ongoing compliance monitoring. Implementing advanced cybersecurity measures, system redundancies, and regular audits can be resource-intensive. For smaller or new DTSPs, these requirements might strain financial resources. 2. Complexity and resource allocation administration, time and effort. The need to establish comprehensive risk management, continuity, and outsourcing frameworks can lead to increased administrative tasks. This includes regular audits, documentation, reporting, and maintaining updated contingency plans. Complying with MAS guidelines requires constant monitoring, updating of protocols, and engagement with third-party vendors. This can divert focus and resources away from core business activities, such as innovation and customer service. 3. Barriers to innovation slowing product development and inelastic processes. Regulatory compliance may slow down the speed of introducing new products or services. For example, every new feature or service might need to go through thorough risk assessments and security checks before launch, which can delay time-to-market. Strict adherence to compliance protocols can lead to less flexibility, potentially stifling creativity. DTSPs might find it challenging to experiment with new technologies or business models that don't neatly fit within the existing regulatory frameworks. 4. Vendor management challenges due to complex arrangements and risk of vendor non-compliance. MAS guidelines require DTSPs to conduct thorough due diligence, create robust contracts, and regularly monitor third-party service providers. Managing these relationships can be challenging, especially when dealing with multiple vendors or international partners. DTSPs can face penalties if their third-party vendors fail to comply with MAS standards. This requires extra vigilance and oversight, adding to the operational burden.
7	Independent Risk Consultant	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>No comment albeit Q2 observations might also be relevant and worth considering.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>Should perhaps be risk-based on the relevant DTSP company's transaction volume, open position, margining requirement/s of various products (including frequency of MTM and margining / close-out call process) given that certain crypto/digital assets have huge price fluctuation on hourly / daily basis.</p>



S/N	Respondent	Responses from respondent
		<p>Further, need of highly reputable digital assets custodian/s to safe-keep / custodise all clients digital assets in properly segregated accounts.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>Proposed duties and responsibilities of CEO, directors and partners of the licensee must be similar if not more stringent than traditional financial service firms given the still developing DTSP sector in products and scale.</p> <p>For new set-ups, it might be prudent to initially require more frequent audit/s say quarterly to ensure all regulatory and internal governance (including onboarding KYC AML / on-off ramp processes), monitoring and reporting, margin call procedures and other risk management and liquidity policy are fully adhered to.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>As below.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>All prior existing customers that were on-boarded prior to obtaining its license must be reviewed and re-affirmed within say 3 months from the license issuance safe from those already permitted under draft FSM notice 6.54 & 6.55.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Reliance of 3rd party must be crystal clear that all responsibilities for compliance under the licensing requirements by MAS will remain with the licensee. Current pre-excluded 3rd party definitions by MAS to be fully observed.</p> <p>Given the current reservation on uneven level of services by some 3rd party service providers for AML/CFT controls and higher ML/TF risks for this sector, it might not be appropriate for this sector to fully rely on 3rd party to perform the services except the interim screening.</p>



S/N	Respondent	Responses from respondent
		<p>In this respect, it should be a requirement that the licensee to have a relevant comprehensive 3rd party outsourcing policy and process should it wish to use such 3rd party services.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>On- / Off-ramp activities from digital or hard wallets in particular cold wallets should perhaps be addressed or they could escape scrutiny by the licensed banks and licensee/s in the absence of such rules per Travel Rules by FATF.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Generally, a DTSP licensee should not be providing pure Correspondent services except to its own clients.</p> <p>Whilst there could be situation that the licensee in trading with its counterparty (which should be separately reviewed / approved), there is no reason for Correspondent services to be provided to said counterparty as such transactions would tantamount to other third party payment transactions which should be out-of-scope and not cover under DTSP license.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>Absolutely no bearer negotiable instruments ie similar to not permitting any third party payments except directly yo the licensee's clients.</p> <p>ps I have reservations on 5.8b to permit payment of smaller cash amount to a recipient or person appointed to act on behalf of a recipient.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p>



S/N	Respondent	Responses from respondent
		<p>These should indeed be fully covered by compliance of FATF rules governing VASPs (our DTSPs) and the required Travel Rule on- / off-ramp activities from wallets.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>Absolutely required and perhaps some additional guidance from current suspicious activities reporting should be further explored or enhanced to cover this growing and challenging sector.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>DTSPs or VASPs operating outside Singapore and not licensed by MAS should not be permitted to operate in SG for their offshore clients and there's absolutely no reason to 'claim' a presence or 'head-quartered' in Singapore if such companies are unwilling to apply for necessary DT services licensing from and subject to regulatory supervision by MAS.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>See comments in Q12.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>Same as Q12.</p>
8	IOTA Foundation	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>We acknowledge the importance of a well-defined and efficient licensing process for DTSPs to ensure regulatory compliance while minimizing administrative burden. The outlined processes and timelines for license application and lapsing provide clarity. However, we suggest further consideration to enhance both the transparency and practicality of these requirements.</p>



S/N	Respondent	Responses from respondent
		<p><u>Application Process and Timelines</u></p> <p>The proposed timeline for license application processing appears reasonable for most DTSPs, but there may be cases where complex business models or cross-border operations require additional time for regulatory approval. We recommend MAS to consider offering a tiered approach to the application process. More specifically:</p> <ul style="list-style-type: none"> • Simplified Procedure: For applicants with simpler business models or those already regulated by other jurisdictions, an expedited review process could help reduce unnecessary delays. • Provisional Licensing: While applications are under review, MAS could consider granting provisional licenses for DTSPs with a track record of compliance in other regulated markets, allowing them to continue operations while full approval is pending. <p><u>Fee Structures and Quantum of Fees</u></p> <p>The proposed licensing fees should reflect the nature and scale of the DTSP’s business. We recommend MAS to consider a tiered fee structure based on the size and scope of the DTSP’s operations. For example:</p> <ul style="list-style-type: none"> • Small-scale DTSPs: Reduced fees or a phased fee model during the first year of operation could encourage innovation and market entry while ensuring regulatory oversight. • Large-scale DTSPs: Higher fees would be appropriate given the larger operational footprint and higher risks associated with more complex business models. <p><u>Lapsing of License</u></p> <p>The six-month inactivity period proposed in Regulation 8 for lapsing of a DTSP’s license may be restrictive for certain providers, especially those whose business cycles are influenced by market trends or seasonal activity. We suggest that MAS introduces more flexibility by allowing DTSPs to apply for temporary suspension of their license during periods of inactivity (e.g., when undergoing major technological upgrades or restructuring).</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>We appreciate the intention behind the proposed minimum financial requirements for DTSPs to ensure that providers are adequately capitalized and able to sustain operations while mitigating risks. We believe there are some areas where refinement could better balance regulatory protection with fostering innovation.</p> <p>The proposed flat \$250,000 base capital for all DTSPs may impose a disproportionate burden on smaller players, start-ups, and emerging companies, potentially stifling innovation in the sector. While we agree that sufficient capital is</p>



S/N	Respondent	Responses from respondent
		<p>essential to ensure the integrity of DTSP operations, a tiered capital requirement based on the scale of the DTSP’s business would be more appropriate. For example:</p> <ul style="list-style-type: none"> • Small-scale DTSPs could be subject to a lower base capital requirement during their initial years (e.g., \$150,000) with a gradual increase as they scale. • Larger and well-established DTSPs with higher volumes or more complex operations could maintain the \$250,000 requirement <p><u>Components of Minimum Financial Requirements</u> The emphasis on maintaining a stable base capital is commendable, but it would be useful to provide more clarity around the liquidity of this capital. Given the nature of the digital token industry, having immediate access to liquid assets is critical for managing sudden operational or market shocks. We recommend a portion of the base capital be held in highly liquid assets (cash or cash equivalents) to ensure quick access in times of stress.</p> <p>Furthermore, we suggest that MAS provides clear guidance on the compositional breakdown of capital. This should include a distinction between fixed capital (e.g., infrastructure investments) and working capital (e.g., cash reserves), ensuring that DTSPs maintain a balance of both to sustain daily operations and long-term growth.</p> <p><u>Ongoing Financial Requirements</u> The ongoing financial requirement is an important component, and it should reflect not only the base capital but also consider the scale and risk exposure of the DTSP’s operations. MAS could consider introducing a risk-weighted approach to ongoing financial requirements, whereby DTSPs handling higher transaction volumes, dealing with higher-risk jurisdictions, or engaging in more complex services may be subject to increased capital requirements. Additionally, MAS could consider requiring DTSPs to demonstrate a buffer or contingency fund that exceeds the minimum capital, especially for those engaged in higher-risk activities. This would ensure resilience during periods of financial stress or market volatility.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>We recognize the critical role that CEOs, directors, and partners play in ensuring the integrity and compliance of DTSPs. That being said, we believe that there are some areas where additional clarity and refinement could improve both governance and the effectiveness of audit requirements.</p> <p><u>Duties of the CEO, Directors, and Partners</u> The CEO's responsibility for the DTSP’s compliance with regulatory obligations is crucial. However, to ensure robust governance and avoid conflicts of interest, it is important to maintain clear checks and balances between operational duties and compliance oversight. We recommend that the compliance function remain</p>



S/N	Respondent	Responses from respondent
		<p>independent of the CEO’s operational control. The compliance officer should report directly to the board of directors or an independent committee, thereby reinforcing accountability and reducing the risk of undue influence or conflicts of interest.</p> <p>Furthermore, to reflect the tiered approach based on the size and complexity of DTSPs, we recommend that the division of duties and governance structures be adaptable to the scale of the business. For larger and more complex DTSPs, governance requirements may include additional layers of oversight, whereas smaller DTSPs with simpler operations could maintain a more streamlined structure.</p> <p>Audit Requirements The frequency of audits should be linked to the size, risk profile, and operational complexity of the DTSP. A tiered approach to audit frequency would ensure that larger or higher-risk DTSPs undergo frequent and rigorous audits, while smaller or lower-risk DTSPs could follow a more standard annual audit process.</p> <p>While annual audits are sufficient for most providers, higher-risk DTSPs may need more frequent external audits or targeted reviews focused on AML/CFT compliance. MAS may also want to consider mandating ad hoc audits in response to significant operational changes, such as mergers, acquisitions, or major technology upgrades.</p> <p>We support the requirement for audits to be conducted by independent third parties, but it’s important to ensure that the auditors have expertise in digital token services and distributed ledger technology. MAS could provide a list of accredited auditors who have the necessary knowledge to assess the unique risks in the digital asset space. This would enhance the quality and relevance of the audits, ensuring they focus on industry-specific issues such as cybersecurity and blockchain governance.</p> <p>To enhance transparency, we propose that MAS require DTSPs to publish a summary of their audit findings in their annual reports or on their websites. This will help build trust with clients and regulators, while providing assurance that key compliance and operational risks are being addressed. Additionally, any material weaknesses or significant deficiencies identified during the audit should be reported directly to MAS, along with the DTSP’s plan to remediate these issues.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>We do not have general comments on the measures proposed in parts 5-8. We would like to highlight that in the rapidly evolving space of digital tokens and blockchain technology, regulatory clarity and flexibility are crucial.</p> <p>We recommend ensuring that proposed measures allow for the development of interoperable systems across different regulatory regimes, particularly as DLT</p>



S/N	Respondent	Responses from respondent
		<p>evolves globally. Also, the regulatory measures should be calibrated to the actual risks posed by different use cases, avoiding a one-size-fits-all approach. Additionally, continuous collaboration with industry stakeholders will be essential in shaping effective regulatory measures that balance innovation with compliance.</p> <p>We remain committed to supporting this dialogue and providing input wherever necessary.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>We do not have general comments on the measures proposed in parts 5-8. We would like to highlight that in the rapidly evolving space of digital tokens and blockchain technology, regulatory clarity and flexibility are crucial.</p> <p>We recommend ensuring that proposed measures allow for the development of interoperable systems across different regulatory regimes, particularly as DLT evolves globally. Also, the regulatory measures should be calibrated to the actual risks posed by different use cases, avoiding a one-size-fits-all approach. Additionally, continuous collaboration with industry stakeholders will be essential in shaping effective regulatory measures that balance innovation with compliance.</p> <p>We remain committed to supporting this dialogue and providing input wherever necessary.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>We believe allowing third-party reliance in the digital token sector is appropriate, provided that safeguards are in place, as outlined in paragraph 11 of the FSM Notice. The ability to rely on third parties that meet AML/CFT standards can streamline operations for DTSPs while maintaining strong regulatory oversight.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>We agree with the proposed amendments in the AML/CFT notices.</p>



S/N	Respondent	Responses from respondent
		<p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Correspondent account services have traditionally been associated with banks and other financial institutions providing services such as facilitating international wire transfers and clearing services on behalf of other financial institutions. In the context of DTSPs, the definition of correspondent account services is appropriately expanded to include the provision of digital token services by one DTSP to another financial institution. Given the global and cross-border nature of many digital token transactions, the proposed requirements for managing correspondent accounts are highly applicable to the sector.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>We agree with the proposal in paragraph 5.8 of the consultation paper and 10 of the draft FSM Notice.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>We agree with the requirements in paragraph 14 of the FSM Notice, which establish comprehensive measures for tracking and documenting digital token value transfers. For effective compliance, we recommend DTSPs adopt automated compliance systems capable of capturing and transmitting essential information—such as the value transfer originator’s and beneficiary’s full names, unique identification numbers, and transaction details—for every value transfer exceeding S\$ 1,500. Furthermore, aligning these requirements with the EU’s Travel Rule would promote consistency with international standards and enhance the traceability of cross-border digital asset transactions.</p>



S/N	Respondent	Responses from respondent
		<p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>We acknowledge the importance of robust reporting requirements for DTSPs to ensure transparency, regulatory oversight, and the mitigation of risks associated with fraud and suspicious activities. The draft notices FSM-N28 and FSM-N29 address critical aspects of reporting, and we offer the following comments and recommendations.</p> <p><u>Reporting of Suspicious Activities and Fraud (FSM-N28)</u> Materiality of Incidents (Paragraph 4) The notice requires DTSPs to report incidents that are "material to the safety, soundness, or reputation of the licensee." We recommend that MAS provide clearer guidelines on what constitutes 'materiality' for DTSPs. For instance, materiality could be defined based on the financial impact, the number of affected customers, or potential reputational damage. This would help DTSPs better assess which incidents warrant formal reporting.</p> <p>Timely Reporting (Paragraph 5) The requirement to lodge a report within 5 working days is appropriate for most incidents. However, in cases where investigations are complex or ongoing, DTSPs should have the option to provide an interim report within the 5-day period, followed by a final, detailed report once the investigation is complete. This would ensure that MAS is informed promptly while allowing DTSPs sufficient time to conduct thorough investigations.</p> <p><u>Submission of Regulatory Returns (FSM-N29)</u> Monthly and Semi-Annual Returns (Paragraphs 6-8) The monthly submission (Form 1A) and semi-annual submission (Form 1B) provide comprehensive coverage of transactions and activities. However, given the high volume of transactions in the digital token space, MAS may consider allowing DTSPs to submit aggregated data for smaller, low-value transactions, especially if they are of low risk. This would reduce the administrative burden on DTSPs while maintaining transparency for larger or higher-risk transactions.</p> <p>Foreign Currency Transactions (Paragraphs 11-12) We support the requirement to report the Singapore dollar equivalent for transactions involving foreign currencies. However, DTSPs often deal with volatile exchange rates. MAS might consider allowing DTSPs to use average monthly exchange rates for reporting, rather than requiring the exact rate at the time of each transaction. Additionally, to avoid unnecessary operational complexity, this reporting process should be fully automated, ensuring accuracy while streamlining the reporting workflow.</p> <p>High-Risk Transactions and Digital Tokens (Paragraph 10 of Form 1B)</p>



S/N	Respondent	Responses from respondent
		<p>The identification and reporting of high-risk transactions (e.g., those involving high-risk jurisdictions or anonymity-enhancing technologies) is critical for AML/CFT compliance. We recommend MAS to use a standardized list of high-risk jurisdictions to ensure consistency across the industry. To streamline this, we recommend considering the utilization of the FATF's list of jurisdictions under increased monitoring (June 2024). Additionally, DTSPs should be required to implement automated monitoring systems that flag transactions involving high-risk digital tokens or jurisdictions, ensuring prompt reporting to MAS.</p> <p>Reporting of Safeguarded Digital Tokens (Paragraphs 3(d), 7(a) of Form 1B) The requirement to report the value of digital tokens safeguarded or administered by the DTSP is crucial for transparency. However, given the fluctuation in digital token values, MAS might consider allowing DTSPs to report the average value of digital tokens held over the reporting period, rather than the value at a specific point in time. This would provide a more accurate reflection of the overall exposure.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>We commend MAS's proactive approach to setting clear and stringent guidelines for technology risk management and cyber hygiene for DTSPs. Below are our comments on these notices, along with some suggestions for refinement.</p> <p><u>Technology Risk Management (FSM-N30)</u> The Notice on Technology Risk Management (FSM-N30) provides a comprehensive framework for ensuring the availability and resilience of critical systems. We fully support the emphasis on identifying critical systems, minimizing downtime, and ensuring swift recovery in the event of a disruption. However, there are a few areas where further clarification and enhancements could be beneficial..</p> <p>Recovery Time Objective (RTO) The stipulated RTO of 4 hours for critical systems is appropriate, especially given the fast-paced nature of digital token markets. However, MAS might consider requiring DTSPs to conduct regular stress tests and disaster recovery drills to validate their ability to meet the RTO in various real-world scenarios (e.g., cyberattacks, system overload, or network failures). Regular testing would ensure that DTSPs are not only theoretically but practically prepared to meet recovery targets.</p> <p>Incident Reporting and Root Cause Analysis The requirement to notify MAS within 1 hour of discovering a relevant incident is a critical safeguard. However, MAS could also consider requiring DTSPs to provide a preliminary incident report within 24 hours of the event, in addition to the 14-day root cause analysis report. This would allow MAS to have early visibility into the incident while ensuring that the full investigation is not rushed. In the root cause analysis report, it may be beneficial to include specific guidelines on the remedial</p>



S/N	Respondent	Responses from respondent
		<p>measures required to prevent recurrence, particularly for systemic issues that may affect other DTSPs as well.</p> <p><u>Cyber Hygiene (FSM-N31)</u> The Notice on Cyber Hygiene (FSM-N31) effectively addresses key cyber hygiene practices that are essential for protecting DTSPs from malicious actors and system vulnerabilities. We support the focus on securing administrative accounts, applying security patches, and implementing multi-factor authentication. However, a few areas could benefit from further elaboration.</p> <p><u>Network Perimeter Defense and Malware Protection</u> The focus on network perimeter defense and malware protection is crucial for mitigating cyber risks. However, MAS could further strengthen these guidelines by requiring DTSPs to implement regular penetration testing of their network perimeter and to establish an ongoing threat monitoring system to detect and respond to potential intrusions in real time.</p> <p><u>Multi-factor Authentication</u> We strongly support the use of multi-factor authentication for administrative accounts and systems that access customer information. MAS could also consider extending this requirement to all user accounts that have access to sensitive operational data or transaction systems, given the risks associated with internal threats and phishing attacks.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>We appreciate the attention to establishing clear conduct, disclosure, and communication standards for DTSPs as outlined in FSM-N32 and FSM-N33.</p> <p><u>Conduct Requirements (FSM-N32)</u> <u>Operating Days and Hours (Paragraphs 17–18)</u> We understand the intent behind requiring DTSPs to operate for a minimum of 10 days a month and 8 hours on each of those days. Given the global nature of digital token services, where DTSPs often serve customers across different time zones, operational demands vary. We recommend MAS to consider allowing DTSPs to design flexible operating hours that suit the specific needs of their customers and the nature of their services. This would ensure that customer support and other essential services are available when needed, without mandating fixed business hours that may not align with customer demand. Additionally, we suggest MAS provide guidance on emergency or non-operating days in unforeseen circumstances such as system outages, cyberattacks, or regulatory investigations. Clear protocols</p>



S/N	Respondent	Responses from respondent
		<p>should be established for informing customers and the MAS about temporary disruptions to operations.</p> <p><u>Disclosure and Communications (FSM-N33)</u> Risk Warning Statement (Paragraph 4 and Annex A) The risk warning statement is clear and comprehensive, emphasizing the potential risks associated with digital token services, including volatility, regulatory limitations, and the possibility of losing funds. We believe this is a critical component of customer protection. However, we suggest that MAS requires DTSPs to tailor risk warnings to specific products or services, especially when dealing with high-risk assets. This would ensure that customers are fully aware of the specific risks associated with each type of service offered. Additionally, to ensure accessibility, MAS could recommend that DTSPs provide risk warnings in multiple languages, particularly for markets where English may not be the primary language of customers.</p> <p>False or Misleading Statements by Third Parties (Paragraph 8) We agree with the requirement that DTSPs take steps to correct false or misleading statements made by third parties about the DTSP’s scope of regulation. However, DTSPs should not be held responsible for all third-party communications, especially in decentralized environments where third-party content can be difficult to monitor. We suggest that MAS provides DTSPs with clear guidance on the actions they are expected to take, such as issuing public corrections or contacting third parties directly. DTSPs should be required to demonstrate reasonable efforts to correct false information but should not be penalized for situations beyond their control.</p> <p>Disclosure of Fees and Exchange Rates (Paragraphs 12–14) The requirement to prominently display exchange rates and fees is essential for fostering trust and transparency. However, given the volatility of the digital token markets, MAS could consider allowing DTSPs to use real-time exchange rate disclosures that are continuously updated. This would provide customers with the most accurate and up-to-date information when conducting transactions. Additionally, we recommend that MAS clarifies how dynamic pricing models (where fees fluctuate based on market conditions) should be disclosed to customers to avoid confusion and ensure compliance.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>We appreciate the intention to apply comprehensive and well-established guidelines to DTSPs under the new regulatory framework.</p> <p><u>Fit and Proper Guidelines (FSG-G01)</u> The Guidelines on Fit and Proper Criteria (FSG-G01) are fundamental to ensuring that individuals and entities responsible for the operations of DTSPs meet the</p>



S/N	Respondent	Responses from respondent
		<p>highest standards of integrity, competence, and professionalism. We support the application of these guidelines to DTSPs. The Guidelines on Risk Management Practices – Technology Risk are highly relevant to DTSPs, which operate in a highly technological and data-driven environment. Cybersecurity, data protection, and system resilience are all critical concerns. We support the application of these guidelines, while also offering the following recommendations.</p> <p>MAS could consider expanding the cybersecurity component of the guidelines to address specific risks associated with digital tokens, such as smart contract vulnerabilities and key management systems. Since many DTSPs interact with distributed systems, there should be clear guidelines on securing these infrastructures.</p> <p>The guidelines should emphasize the importance of a robust incident response plan, particularly in the event of cyberattacks, system failures, or breaches that could impact customers or the broader financial system. Given the 24/7 nature of digital asset markets, DTSPs must have strong contingency plans that prioritize quick recovery and minimal disruption.</p> <p>We also strongly support the application of the Guidelines on Business Continuity Management to DTSPs. The digital asset space is volatile, making strong business continuity plans crucial for maintaining operations during unforeseen disruptions.</p> <p>Lastly, for DTSPs engaged in innovative and experimental technologies, MAS could consider creating a regulatory sandbox framework within the guidelines. This would allow DTSPs to test new business models and technologies in a controlled environment, while still adhering to core regulatory principles.</p>
9	Notabene	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>Notabene appreciates the clarity MAS provides in setting out the application processes, timelines, and fee structures for Digital Token Service Providers (DTSPs) under the FSM Act. Here are our comments and suggestions:</p> <ol style="list-style-type: none"> 1. License Application and Timelines: The processes for license application outlined in regulations 3 to 6 appear straightforward and well-structured, providing clear guidelines for DTSPs to follow. However, a recommended addition would be a preliminary guidance phase where potential applicants can seek preliminary feedback on their readiness before the full application. This could reduce application resubmissions and streamline approval timelines. 2. Lapsing of Licenses: Regulation 8’s provision for license lapsing after a six-month cessation period is reasonable in preventing dormant licenses. Nevertheless, the inclusion of a notification period (e.g., 30 days before



S/N	Respondent	Responses from respondent
		<p>lapsing) would help ensure that DTSPs are adequately informed and prepared to either resume services or formally exit the market. This could prevent unintended lapses and improve compliance.</p> <p>3. Fee Structures and Quantum of Fees: The annual license and application fees, as proposed, align with industry standards. However, providing a tiered fee structure based on DTSPs’ service scale or transaction volumes could offer more equitable financial obligations, particularly for smaller or emerging service providers. Additionally, early-stage fee reductions for new DTSPs could incentivize innovation in the sector while maintaining regulatory compliance.</p> <p>In summary, we support the proposed licensing processes, timelines, and fees but recommend additional measures to accommodate flexibility for new entrants and improve compliance transparency for existing licensees.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>No comment.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>In response to the Monetary Authority of Singapore’s consultation on the duties of CEOs, directors, and partners of licensees, as well as the proposed audit requirements for digital token service providers (DTSPs), we would like to offer the following comments:</p> <ol style="list-style-type: none"> 1. Duties of CEO, Directors, and Partners of the Licensee: Notabene supports MAS’s focus on accountability and governance at the executive level for DTSPs. Clearly defined responsibilities for the CEO, directors, and partners help ensure robust oversight and alignment with regulatory expectations, particularly given the high compliance standards expected for AML/CFT measures within the crypto sector. We humbly suggest that MAS consider explicitly incorporating risk management responsibilities into these duties, especially concerning AML/CFT obligations, operational resilience, and cybersecurity. This would align the executive role with the unique risk profile of DTSPs and the emerging regulatory landscape surrounding digital assets. Additionally, requiring periodic training on compliance and risk management for key officers could further strengthen the governance framework and enhance responsiveness to regulatory updates, such as those concerning the Travel Rule. 2. Audit Requirements: Notabene agrees that comprehensive audit requirements are essential for maintaining financial integrity and transparency among DTSPs. Audits not only verify compliance but also reinforce internal controls that can



S/N	Respondent	Responses from respondent
		<p>detect potential risks proactively. We humbly suggest that MAS may consider establishing a specific audit framework or set of standards tailored to DTSPs, particularly around transaction monitoring, Travel Rule compliance, and cybersecurity controls. This approach would ensure that audits are meaningful and aligned with the specific operational and regulatory risks faced by DTSPs. To facilitate smoother compliance, MAS might also provide clarification on acceptable external audit qualifications for firms conducting these audits, ensuring that auditors have expertise in the unique dynamics of digital token services and regulatory obligations like the Travel Rule.</p> <p>We believe that establishing clear, consistent, and targeted duties and audit standards for DTSP executives will promote compliance, strengthen market confidence, and support the development of a resilient digital asset ecosystem in Singapore.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>Notabene commend's the Monetary Authority of Singapore (MAS) for proposing a comprehensive and detailed regulatory approach for Digital Token Service Providers (DTSPs) under the Financial Services and Markets Act 2022. Our comments focus on the alignment of these notices and guidelines with international standards, particularly in light of Financial Action Task Force (FATF) Recommendations, including the Travel Rule.</p> <p><u>Part 5: Anti-Money Laundering and Countering the Financing of Terrorism (FSM-N27)</u></p> <p>We acknowledge the emphasis on AML/CFT measures in FSM-N27, specifically the requirement for DTSPs to implement robust customer due diligence (CDD) and monitoring systems. Notably, the Travel Rule provisions are critical for achieving compliance with FATF Recommendations, which mandate DTSPs to gather and transmit originator and beneficiary information for digital token transfers.</p> <p>Our observations on FSM-N27 are as follows:</p> <ol style="list-style-type: none"> 1. Alignment with Global Standards: Given the cross-border nature of digital token services, ensuring that the FSM-N27 provisions align with the FATF's Travel Rule requirements will facilitate Singapore's integration into the global compliance ecosystem. DTSPs would benefit from MAS guidance on data-sharing protocols and technology solutions that could support seamless information transfers. 2. Data Privacy and Security: Implementing the Travel Rule presents challenges in data privacy and security, as DTSPs must safeguard transmitted data while meeting AML/CFT obligations. We encourage MAS to provide additional guidelines or best practices to ensure secure data handling and storage.



S/N	Respondent	Responses from respondent
		<p><u>Part 8: Guidelines on Fit and Proper Criteria (FSG-G01)</u> The Fit and Proper Criteria outlined in FSG-G01 are essential to maintaining industry integrity. We suggest additional guidance on the qualifications and competencies expected from DTSP personnel, particularly in AML/CFT compliance roles.</p> <p>In summary, we appreciate MAS’s proactive approach to regulating DTSPs and addressing AML/CFT risks associated with digital token services. A transparent, robust regulatory framework will enhance market integrity, strengthen compliance, and bolster Singapore’s position as a global leader in digital finance.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>No comment.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>In response to MAS’s proposal on permitting licensees to rely on third parties for Customer Due Diligence (CDD) measures, Notabene recognizes the operational efficiency this approach can provide, yet underscore the critical importance of robust due diligence in managing risks associated with digital assets, especially under the Travel Rule. Given the unique ML/TF vulnerabilities in this sector, it is vital that third-party reliance aligns closely with FATF standards and meets the expectations of cross-border compliance.</p> <p>General Comments on Third-Party Reliance for Digital Token Service Providers and Travel Rule Compliance:</p> <ol style="list-style-type: none"> 1. AML/CFT Standards, FATF Compliance, and VASP Due Diligence: While third-party reliance offers potential efficiencies, it is essential that any third party being relied upon is consistently and rigorously supervised for AML/CFT compliance in line with FATF standards, particularly with respect to Virtual Asset Service Providers (VASPs). Given that FATF acknowledges the need for jurisdictions to treat VASPs from countries without effective licensing or registration frameworks as high-risk, licensees must incorporate heightened scrutiny and due diligence measures for such entities. This is particularly relevant under the Travel Rule, where reliance on third parties necessitates secure, prompt, and traceable data-sharing practices to meet CDD obligations. 2. Risk-Based Assessment of Jurisdictions with High-Risk VASPs: While MAS’s proposal requires licensees to assess ML/TF risks associated with the jurisdictional exposure of third parties, additional guidance specific to VASPs



S/N	Respondent	Responses from respondent
		<p>could further strengthen compliance. As FATF recommends treating VASPs from jurisdictions lacking robust licensing frameworks as high-risk, MAS could enhance its guidance on jurisdictional factors that licensees should consider when evaluating these third-party VASPs. This would assist licensees in adopting a consistent and effective risk-based approach to identify and manage cross-border ML/TF risks.</p> <p>3. Immediate Data Access for Compliance with Travel Rule Obligations: We strongly support MAS’s requirement that third parties provide timely access to all relevant CDD data. In the context of the Travel Rule, where accurate originator and beneficiary information is crucial to meeting cross-border compliance standards, the ability to obtain immediate and verifiable data is essential to managing ML/TF risks and ensuring traceability of digital asset transfers.</p> <p>In summary, we agree that third-party reliance can be appropriate for the digital token service sector if it includes rigorous due diligence, robust Travel Rule compliance, jurisdictional risk assessment, and data accessibility provisions. We humbly recommend that MAS maintain an adaptable framework for third-party reliance, allowing for reassessment as industry and regulatory AML/CFT standards continue to evolve.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>No comment.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Notabene supports MAS’s proposed measures to require licensees to implement risk mitigation procedures when offering or engaging in correspondent account services with another financial institution. Ensuring that robust AML/CFT standards are maintained at all points in the financial chain is essential, particularly for sectors where the inherent risks are heightened by the nature of digital token services.</p> <p>Regarding the specific provisions:</p> <ol style="list-style-type: none"> 1. Assessing Suitability of Financial Institutions (5.7a): In addition to assessing the AML/CFT controls of correspondent financial institutions, DTSPs could also evaluate the Travel Rule compliance measures of their counterparties. This includes verifying that counterparties have processes in place for transmitting originator and beneficiary information for virtual asset transfers, as required under FATF standards. Ensuring alignment on Travel Rule compliance could



S/N	Respondent	Responses from respondent
		<p>reduce exposure to risks associated with unregulated entities or jurisdictions with weak Travel Rule adherence.</p> <ol style="list-style-type: none"> 2. Documenting AML/CFT Responsibilities (5.7b): In defining AML/CFT responsibilities, DTSPs could explicitly document each party’s obligations regarding the Travel Rule. This would help delineate accountability in instances of non-compliance or incomplete data sharing, providing clarity in inter-institutional data transmission protocols and strengthening AML/CFT safeguards. 3. Senior Management Approval (5.7c): When approving new correspondent account relationships, senior management should also consider the prospective institution’s Travel Rule compliance as part of the risk assessment. Given the challenges of data sharing in cross-border transactions, assessing how a correspondent institution meets Travel Rule standards could form an essential aspect of the decision-making process. <p>Incorporating the Travel Rule as a key part of correspondent account services would align MAS’s standards with global AML/CFT expectations, ensuring more thorough risk mitigation and promoting regulatory harmony in digital token services.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>No comment.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>The value transfer requirements in Paragraph 14 of FSM-N27 align well with the FATF Travel Rule, which similarly mandates the collection, transmission, and retention of originator and beneficiary information for digital asset transactions. Notabene humbly suggests clear and prescriptive guidance on what is “reasonable measures” for information collection and transaction processing actions which will support DTSPs in meeting these requirements, similar to practices under the EU Transfer of Funds Regulation.</p> <ol style="list-style-type: none"> 1. Relevant Information for Law Enforcement Purposes



S/N	Respondent	Responses from respondent
		<p>Including the full range of Travel Rule-compliant information will enhance cross-border information compatibility and align with international AML/CFT norms. For effective law enforcement, DTSPs should collect and transmit:</p> <ul style="list-style-type: none"> • Value Transfer Originator and Beneficiary Information: As required by the Travel Rule, this should include legal name, unique identifier (e.g., passport or government ID number for individuals or business registration number for entities), date of birth (for individuals), and jurisdiction. • Transaction-Specific Information: Transaction date, time, digital token type, value amount, transaction ID, and wallet addresses. This information allows for precise transaction reconstruction and origin tracing, which is crucial for cross-border cooperation and enforcement. <p>2. Defined Reasonable Measures and Prescriptive Guidance To meet the MAS requirements for “reasonable measures,” clear, standardized criteria should guide DTSPs on verification procedures. We recommend that MAS provide specific guidance on:</p> <ul style="list-style-type: none"> • Reasonable Verification Measures: Detailed criteria for originator identity verification to ensure consistency, such as acceptable forms of identification and validation processes. For example, alignment with the EU TFR’s prescriptive standards would help establish minimum documentation requirements. • Execution, Rejection, or Suspension Criteria: Explicit guidance on handling transfers with missing or incomplete information, such as: • Thresholds for Rejection: Defining circumstances where information deficiencies warrant a transfer block or require remediation. • Risk-Based Controls: Guidelines on when to apply enhanced due diligence based on transaction risk (e.g., higher thresholds for high-risk jurisdictions). <p>These elements will empower DTSPs to act with confidence, especially for complex, high-risk transactions, while ensuring they meet regulatory expectations.</p> <p>3. Operationalization and Industry Initiatives Adopting industry-wide initiatives aligned with the Travel Rule will streamline compliance across DTSPs. We recommend a formalized "Escalation and Reporting Guidelines" in that MAS could develop specific escalation criteria for when and how DTSPs should alert law enforcement or other entities of suspicious activities, promoting consistency in enforcement and enabling effective, timely investigations.</p> <p>Incorporating Travel Rule standards and prescriptive guidance on “reasonable measures” and transfer handling will empower DTSPs to implement MAS’s value transfer requirements effectively. Establishing clear guidelines for information handling, verification, and action thresholds will further Singapore’s regulatory alignment with the EU TFR, creating a consistent, reliable framework for cross-border digital asset transfers.</p>



S/N	Respondent	Responses from respondent
		<p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>On FSM-N28 (Notice on reporting of suspicious activities and incidents of fraud): Notabene supports the initiative to mandate prompt reporting of suspicious activities and fraud incidents. For effective compliance, we suggest clarifying what constitutes a “material” incident for a DTSP’s safety, soundness, or reputation. Clear thresholds or examples could prevent under-reporting and ensure that reporting requirements are uniformly understood and applied across the industry. Additionally, it would be beneficial to specify timeframes for reporting, ensuring alignment with industry standards for immediate incident reporting to regulatory bodies.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>Thank you for the opportunity to provide comments on the draft FSM-N30 and FSM-N31. Few points to consider:</p> <ol style="list-style-type: none"> 1. Critical Systems and Downtime: <ul style="list-style-type: none"> • The requirements to minimize unscheduled downtime for critical systems and to establish a recovery time objective of 4 hours reflect the essential need for operational continuity. However, given the complex and evolving nature of distributed ledger technology (DLT), especially when DTSPs depend on third-party networks, we recommend MAS consider a flexible approach. Allowing for specific exceptions or the use of alternative failover protocols in critical situations could further strengthen resilience without adversely impacting service delivery. 2. Incident Reporting Timelines: <ul style="list-style-type: none"> • The 1-hour notification requirement upon discovering a severe system malfunction or cybersecurity incident demonstrates MAS’s commitment to prompt regulatory oversight. However, ensuring compliance with this timeline may pose challenges in situations requiring rapid internal assessment before full reporting. A two-tiered notification approach might be more effective, where a preliminary notification is made within the first hour, followed by a detailed update within a 24-hour window, with the final root cause analysis due within 14 days. 3. Customer Information Protection: <ul style="list-style-type: none"> • Protecting customer data is paramount. The requirement for IT controls to safeguard information from unauthorized access aligns well with global best practices. We would suggest expanding the scope to include recommendations



S/N	Respondent	Responses from respondent
		<p>for continuous monitoring and regular risk assessments, as this could enhance DTSPs’ ability to proactively detect and mitigate potential breaches.</p> <p>Additional Recommendation on Global Alignment: MAS’s approach aligns with international regulatory trends, such as the EU’s Digital Operational Resilience Act (DORA), which similarly emphasizes operational resilience, incident reporting, and strict cybersecurity controls. By drawing on such global standards, MAS can ensure DTSPs operating in Singapore meet internationally recognized benchmarks, facilitating seamless compliance for entities operating across jurisdictions. We recommend MAS consider referencing DORA’s resilience standards as a means of aligning Singapore’s regulatory environment with global best practices in operational resilience and cybersecurity.</p> <p>This comparison can strengthen the case for MAS’s approach by illustrating its alignment with other leading regulatory frameworks. Overall, the draft requirements under FSM-N30 and FSM-N31 underscore the importance of rigorous technology risk management and cyber hygiene. We commend MAS for its commitment to security and resilience in the digital token sector.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>No comment.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>In Notabene's response to Question 14, regarding the application of the guidelines outlined in paragraphs 8.1 and 8.2 to licensees, we submit the following considerations:</p> <ol style="list-style-type: none"> 1. Application of Fit and Proper Criteria: We support the amendment of Guideline No. FSG-G01 to include all Digital Token Service Providers (DTSPs) under the Fit and Proper Criteria. Given the increasing complexity and associated risks in the digital token space, it is essential that licensees meet robust standards for integrity, competency, and financial soundness. However, we recommend clarifying the criteria’s application to licensees who may have dual roles as intermediaries and service providers to minimize ambiguity around role-specific requirements. 2. Relevance of Existing Risk Management and Outsourcing Guidelines: We agree that the Guidelines on Risk Management Practices – Technology Risk, Business



S/N	Respondent	Responses from respondent
		<p>Continuity Management, and Outsourcing remain relevant and should apply to all licensees, including DTSPs. These guidelines are critical to managing technology risk, safeguarding operational resilience, and ensuring sound outsourcing practices, all of which are fundamental for service continuity and maintaining client trust in the DTSP sector.</p> <p>3. Specificity for DTSPs in Risk Management: Considering the unique risk landscape faced by DTSPs—such as cybersecurity threats and technology dependencies—we humbly recommend that MAS consider developing addendums or sector-specific examples within the existing guidelines to provide DTSPs with practical, scenario-based guidance. This could further strengthen DTSPs’ ability to implement effective risk management practices while aligning with MAS’s broader regulatory framework.</p> <p>4. Alignment with Global Standards: Given that DTSPs often operate internationally, aligning these guidelines with global standards, such as those from FATF, can enhance cross-border consistency and facilitate compliance for multinational licensees. This is especially relevant as global regulatory convergence around digital assets and AML/CFT obligations continues to evolve, including adherence to the Travel Rule and related information-sharing protocols.</p> <p>In summary, while we agree with extending the guidelines to all licensees, further clarity and tailored guidance for DTSPs would promote effective compliance and risk management in this emerging sector. We appreciate MAS’s proactive approach to fostering a secure and resilient digital asset ecosystem and welcome further dialogue to address sector-specific needs.</p>
10	Respondent A	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>[Confidential].</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>[Confidential].</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>The Proposed FSM Regulations detail the approval requirements for CEOs, directors, and partners of digital token service providers (DTSPs), as well as audit expectations. These elements are crucial for ensuring that DTSPs operate with strong governance,</p>



S/N	Respondent	Responses from respondent
		<p>transparency, and accountability, particularly given the sector’s regulatory and financial risks.</p> <p><u>Approval and Duties of Senior Officers (Regulation 10)</u> The requirement for CEOs, directors, and partners to obtain MAS approval ensures that individuals in these roles meet high standards of competence, integrity, and sound financial judgment. This aligns with MAS’s overall goal of safeguarding the industry’s reputation and stability. The stringent approval process is particularly important for the digital token sector, where regulatory compliance, operational risks, and cross-border transactions require sophisticated governance.</p> <p>MAS might consider enhancing these criteria by explicitly requiring sector-specific qualifications, such as experience in financial services, digital assets, and risk management. Furthermore, creating a streamlined pathway for experienced candidates with a proven compliance history could balance regulatory rigor with efficient onboarding. By specifying industry-relevant qualifications, MAS would set clear standards that strengthen DTSP governance, supporting a regulatory environment that values both rigor and agility.</p> <p><u>Audit Requirements for Licensees (Regulation 11)</u> The audit requirements outlined in Regulation 11, which mandate the submission of audit reports within six months of the fiscal year’s end, provide essential oversight. Requiring the auditor’s contact details and signature further ensures accountability and transparency. However, given the fast-paced digital token industry, it may be beneficial for DTSPs to adopt continuous auditing and monitoring practices beyond the annual requirement.</p> <p>MAS might encourage licensees to conduct additional, risk-based internal audits, particularly in areas such as cybersecurity, AML/CFT compliance, and transaction monitoring. Periodic reporting on these high-risk areas could supplement the annual audit and allow MAS to proactively address emerging risks.</p> <p>Incorporating risk-based audits would enable DTSPs to maintain compliance with evolving industry standards while providing MAS with more timely data for regulatory review. This would enhance the overall resilience and adaptability of the sector.</p> <p><u>Documentation and Record-Keeping</u> The requirement to document and submit audit findings is key to ensuring that DTSPs maintain high standards of record-keeping and compliance. Given the importance of transparency in regulatory oversight, robust documentation practices will be essential for managing compliance and facilitating MAS audits.</p> <p>To improve efficiency, MAS could provide guidelines on the preferred format and structure for audit reports, which would help DTSPs standardize their submissions and support timely, consistent regulatory review. Standardized documentation</p>



S/N	Respondent	Responses from respondent
		<p>would reduce administrative burdens, allowing DTSPs to allocate resources efficiently while ensuring comprehensive compliance with MAS’s requirements.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>[Confidential].</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>The requirement for digital token service providers to apply customer due diligence (CDD) to existing customers, or “Pre-License Customers,” upon obtaining a DTSP license is a crucial step for maintaining consistent AML/CFT standards across the board. This requirement aligns with international best practices by ensuring that all customers are subject to the same level of scrutiny, regardless of their onboarding timeline.</p> <p><u>Timeframe for Implementation</u> A clearly defined timeframe for completing CDD on Pre-License Customers would assist licensees in prioritizing compliance activities effectively, minimizing disruptions while meeting regulatory expectations. A phased approach based on the risk profile of customers could enhance efficiency, allowing DTSPs to focus initial efforts on high-risk customers before addressing lower-risk segments. MAS could consider specifying a risk-based timeframe (e.g., a three-to-six-month period), allowing licensees to first apply CDD to customers assessed as higher-risk, ensuring that resources are allocated in proportion to potential ML/TF risks.</p> <p><u>Adjustments for Changes in CDD Requirements (Paragraph 6.55)</u> MAS’s guidance allowing DTSPs to exercise materiality and risk-based judgment when reassessing existing customers following changes to CDD measures is a balanced and flexible approach. It acknowledges the variability in customer profiles and ensures that enhanced measures are applied where needed, reducing unnecessary compliance burdens. For transparency and consistency, MAS could provide an indicative list of factors for determining materiality and risk, such as transaction volume, geographic factors, and historical customer behavior. This would assist DTSPs in developing a standardized methodology for assessing when to re-apply CDD.</p> <p><u>Data Adequacy and Documentation</u> The allowance for DTSPs to consider the adequacy of existing data and documents when revisiting CDD measures for existing customers promotes a practical approach to compliance, avoiding redundant data collection while maintaining rigorous standards. This is especially relevant in the fast-paced digital token space, where</p>



S/N	Respondent	Responses from respondent
		<p>streamlined operations are essential. MAS could clarify that documentation from initial CDD can be reused if it remains valid and current, while indicating situations in which updates are expected, such as significant changes in a customer’s transaction behavior or risk profile.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>The option for digital token service providers to rely on third parties for customer due diligence (CDD) measures is an appropriate and necessary measure to support scalability and efficiency in the sector. However, the framework must be designed to ensure robust AML/CFT compliance, given the sector’s susceptibility to cross-border risks and evolving regulatory standards.</p> <p><u>Suitability of Third-Party Reliance</u> Allowing reliance on third parties aligns with the operational needs of digital token providers, who often operate in multiple jurisdictions and require scalable compliance solutions. Relying on vetted third parties, especially those supervised for AML/CFT measures consistent with FATF standards, can provide efficiency without compromising compliance. MAS could enhance safeguards by requiring DTSPs to conduct a periodic reassessment of the third-party’s AML/CFT compliance status, particularly for third parties operating in higher-risk jurisdictions or subject to varying regulatory oversight. This would ensure that DTSPs maintain control over evolving risks within the third-party landscape.</p> <p><u>Preclusion of Certain License Holders</u> The decision to preclude reliance on payment services license holders or equivalent entities reflects the varying AML/CFT standards across the payments sector, which may not align with the rigorous requirements needed for digital token services. This approach underscores MAS’s commitment to minimizing ML/TF risks within the digital asset sector. MAS could consider allowing DTSPs to rely on payment services license holders, but only if they meet enhanced AML/CFT criteria and demonstrate robust compliance practices. This flexibility would enable DTSPs to leverage high-standard providers within the payments sector, thus supporting a more cohesive compliance ecosystem.</p> <p><u>Documentation and Ongoing Monitoring</u> The requirements for DTSPs to document the basis of their reliance and obtain CDD information immediately upon request ensure accountability and transparency. However, as MAS prohibits reliance on third parties for ongoing monitoring, it is critical for DTSPs to have systems in place that integrate third-party data effectively into their own monitoring frameworks. MAS might consider allowing DTSPs to rely</p>



S/N	Respondent	Responses from respondent
		<p>on third parties for transaction screening and alerting, provided that the DTSP retains full oversight and final decision-making authority. This flexibility would support operational efficiency while ensuring that DTSPs uphold their AML/CFT obligations without diluting control.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>The proposed amendments to exclude licensees, and similarly regulated entities, from the definition of a “third party” for AML/CFT reliance purposes reflect MAS’s proactive stance in maintaining stringent AML/CFT standards across the financial ecosystem. Excluding these entities from reliance eligibility addresses potential gaps in compliance levels and risk management, particularly given the heightened ML/TF risks associated with digital token service providers and certain payment service providers.</p> <p>The decision to exclude digital token service providers and certain payment service licensees from being eligible third parties ensures a higher standard of AML/CFT compliance within the sector. Licensees and payment services providers often operate in high-risk domains and, as such, may not meet the stringent AML/CFT controls required by more traditional financial institutions. To further enhance this framework, MAS could consider allowing reliance on these excluded entities in instances where they meet enhanced AML/CFT requirements verified through a certified audit or compliance review. This would provide flexibility for financial institutions needing specialized CDD support while maintaining high compliance standards.</p> <p><u>Restrictions on Intragroup Reliance</u> The proposed restriction on financial institutions relying on their own branches, subsidiaries, and related corporations holding only a payment services license or digital token service provider license effectively mitigates intra-group risk spillovers. By ensuring that AML/CFT compliance is consistently applied across all units, MAS strengthens the overall resilience of Singapore’s financial sector. MAS might allow intragroup reliance under controlled conditions, such as for entities that can demonstrate equivalent or higher AML/CFT standards and are subject to frequent internal audits. This would allow groups to leverage compliance resources effectively while mitigating risks through regular assessments and controls.</p> <p><u>Clarification on Foreign-Supervised Entities</u> Allowing reliance on foreign-supervised entities holding multiple financial services licenses, beyond just payment services or digital token provider licenses, aligns with global best practices. It enables financial institutions to work with foreign entities</p>



S/N	Respondent	Responses from respondent
		<p>that are subject to comprehensive regulatory oversight, thus supporting cross-border efficiency without compromising AML/CFT standards. MAS could provide guidelines for assessing the adequacy of foreign AML/CFT supervision, including factors such as the foreign jurisdiction’s regulatory reputation, alignment with FATF standards, and historical compliance record. This would help financial institutions make informed decisions when relying on foreign entities.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>The proposed requirements for Correspondent Account Services (CAS) in paragraph 5.6 of the draft FSM Notice are both applicable and appropriate for the digital token service provider (DTSP) sector. Given the inherent cross-border nature and rapid transactions within digital token services, the FATF-aligned risk mitigation measures ensure that DTSPs are aligned with global AML/CFT standards, providing a secure framework for correspondent services while addressing potential ML/TF risks.</p> <p><u>Applicability of Risk Mitigation Measures</u> The requirement for DTSPs to assess the suitability of financial institutions when providing or receiving CAS, including evaluating their AML/CFT controls, is essential for preventing potential misuse of these services. The dynamic and often cross-jurisdictional interactions in digital token services make these standards particularly relevant to ensuring consistent risk management. MAS could consider offering guidance on specific factors DTSPs should evaluate, such as transaction monitoring capabilities and the jurisdiction’s regulatory reputation, to better equip licensees in applying a comprehensive assessment.</p> <p><u>Documentation of AML/CFT Responsibilities</u> Documenting the respective AML/CFT responsibilities between the DTSP and the financial institution adds clarity and supports accountability in CAS relationships. This approach ensures that both parties maintain a shared understanding of their obligations, which is critical for consistent compliance across jurisdictions. MAS might provide a template or checklist for documenting these responsibilities to assist DTSPs in maintaining comprehensive records. This would support efficiency while ensuring that all essential compliance areas are consistently covered.</p> <p><u>Senior Management Approval</u> Requiring senior management approval for establishing new CAS relationships is a prudent step, emphasizing the strategic importance of such relationships and ensuring that high-level oversight is applied to CAS-related risks. MAS could suggest criteria for senior management reviews, such as the financial institution’s risk rating, previous compliance records, and anticipated transaction</p>



S/N	Respondent	Responses from respondent
		<p>volumes. Establishing these review standards would promote consistent decision-making processes at the senior management level.</p> <p><u>Prevention of Shell Financial Institutions</u> The stipulation that DTSPs must avoid CAS relationships with shell financial institutions and must ensure that their financial institution counterparts do not engage shell institutions aligns with global best practices. This measure effectively reduces the risk of facilitation of ML/TF activities through CAS relationships. MAS could reinforce this requirement by encouraging DTSPs to periodically review and update their CAS-related risk assessment frameworks, incorporating recent data on higher-risk jurisdictions and entities. This approach would ensure that the anti-shell institution policy remains effective as regulatory environments evolve.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>[Confidential].</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>The value transfer requirements for digital token services are critical for ensuring transparency and traceability, especially for law enforcement purposes. The information accompanying value transfers should be comprehensive enough to support AML/CFT efforts while also being feasible for digital token service providers (DTSPs) to implement consistently across varied platforms.</p> <p><u>Key Information for Law Enforcement</u> Essential Data Points: For law enforcement purposes, it is crucial that each value transfer includes the following information:</p> <p>Value Transfer Originator and Beneficiary Names: Identifying both parties involved in the transfer.</p> <p>Unique Identification Numbers: Such as government-issued IDs for individuals or business registration numbers for entities, to ensure precise tracking.</p>



S/N	Respondent	Responses from respondent
		<p>Transaction Reference Number: Ensuring each transaction is traceable across the DTSP’s systems and any intermediary institutions.</p> <p>Details of the Digital Token: Including type, amount, and transaction date, providing a full picture of the transfer.</p> <p>Rationale: These data points give law enforcement critical information for investigations while minimizing excessive data collection. The inclusion of a transaction reference number allows easy cross-referencing in case of audits or inquiries, promoting efficient traceability.</p> <p><u>Record-Keeping Requirements</u></p> <p>Long-Term Retention: Records should be maintained for at least five years, aligning with international standards and ensuring data is available for potential investigations.</p> <p>Types of Records to Retain: Full Transaction Records: Including the information listed above, along with any additional data required for compliance purposes.</p> <p>Audit Trails for Data Requests: Documentation showing how information was shared with law enforcement or other authorities, ensuring transparency and accountability.</p> <p>Suggestion: MAS could issue specific guidance on formatting and storing this data, such as maintaining both digital and physical (if applicable) copies of records, to ensure compliance consistency across DTSPs.</p> <p><u>Operationalizing Requirements in Practice</u></p> <p>Standardized Data Transmission Protocols: Implementing industry-wide standards, such as the ISO 20022 messaging format, for transferring information across platforms could help DTSPs ensure that all required information is consistently transmitted, even when involving multiple intermediaries.</p> <p>Blockchain Solutions for Traceability: For value transfers involving digital tokens, blockchain-based solutions could enhance record traceability. Immutable ledgers allow DTSPs to securely record transaction details, thereby meeting traceability requirements while safeguarding data integrity.</p> <p>Centralized Reporting System: An industry-wide initiative to create a secure, centralized database for storing value transfer information (with access controls) could assist DTSPs in securely maintaining and sharing records with MAS or law enforcement. This repository could be used for secure storage and timely retrieval of transaction data as needed for investigations.</p> <p><u>Examples of Industry-Wide Initiatives</u></p>



S/N	Respondent	Responses from respondent
		<p>Collaborative Blockchain Consortia: DTSPs could join consortia aimed at developing blockchain protocols that standardize how value transfer data is stored and transmitted across participants. Such consortia could also establish governance standards, ensuring all members adhere to a unified compliance approach.</p> <p>Real-Time Monitoring Systems: While many DTSPs already utilize real-time monitoring systems, these solutions may need to be calibrated specifically to MAS’s requirements, such as maintaining traceability for law enforcement and ensuring comprehensive coverage of originator and beneficiary information. For DTSPs handling high transaction volumes and cross-border transfers, real-time monitoring allows for immediate detection of any incomplete or missing data, which supports proactive compliance without disrupting the transaction flow. This approach ensures that DTSPs not only continue meeting MAS’s standards but also stay prepared for evolving regulatory expectations.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>[Confidential].</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>[Confidential].</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>[Confidential].</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>The application of the Guidelines on Fit and Proper Criteria (FSG-G01) to all licensees under the DTSP Provisions is a necessary and prudent step to ensure that individuals in key positions within digital token service providers (DTSPs) adhere to high standards of integrity, competence, and financial soundness. Given the distinct risks and complexities associated with the digital token sector, extending these</p>



S/N	Respondent	Responses from respondent
		<p>guidelines will enhance the regulatory framework’s robustness and promote responsible governance.</p> <p><u>Relevance of Fit and Proper Criteria for DTSPs</u> The extension of the fit and proper guidelines to DTSP licensees aligns well with MAS’s objectives to uphold industry standards across all regulated entities. DTSPs, due to their involvement in digital assets and cross-border transactions, face unique operational and compliance challenges. Applying these guidelines ensures that individuals in senior positions within DTSPs meet the same rigorous standards expected of other financial institutions, fostering industry-wide trust and stability. MAS could consider enhancing the guidelines to include sector-specific competencies for DTSP leadership, such as digital asset risk management, AML/CFT practices related to digital transactions, and cybersecurity expertise. This adjustment would ensure that DTSP executives possess the specialized knowledge necessary to navigate the unique risks inherent in this sector.</p> <p><u>Clear Expectations for Compliance with Fit and Proper Criteria</u> The "Guidelines on Fit and Proper Criteria" place the onus on licensees to demonstrate their suitability, which is appropriate for establishing accountability. DTSPs may benefit from more detailed guidance or templates that clarify how to document and demonstrate compliance with the guidelines, particularly for criteria that may be applied differently in the digital token sector.</p> <p>MAS could provide a standardized self-assessment form or checklist that DTSPs can use to assess and document their compliance with the fit and proper criteria. This approach would help ensure consistency across DTSPs and streamline the review process for MAS, making it easier to evaluate adherence to the guidelines.</p>
11	Respondent B	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <ol style="list-style-type: none"> 1. The lapse of DTSP license after 6 months if the licensee has ceased to carry on business in providing all of the DT services authorized is reasonable. However, the difficulty lies in the tracking and enforcement as there is no requirement for the licensee to inform MAS that it has ceased the authorized DT services. 2. As a suggestion, it would be useful to give license applicant some estimated indication of the duration MAS will take to process the application based on the assumption that all information submitted are in order and the various processes the applicant will have to go through. 3. Another comment is that without a transitional arrangement, the DTSP only have 4 weeks' notice before the commencement of the FSM Act. This timeline is definitely insufficient for the DTSP to prepare and apply for a license. Even if the DTSP managed to apply within the 4 weeks' notice period, it is unlikely their license will be approved by MAS within the period. This essentially means that existing DTSP players are forced to suspend or cease operations once the FSM



S/N	Respondent	Responses from respondent
		<p>Act takes effect. These could cause severe disruption to DTSPs, resulting in mass layoffs of their staff based in Singapore, possibly also having downstream effects on the service providers in Singapore engaged by DTSPs. As mentioned in last sentence of paragraph 2.8 of the consultation paper, MAS can give exemption once the FSM Act take effect. Would MAS considers providing an exemption to those who are currently operating and have applied for a DTSP within a certain period to continue to operate until the license is approved or rejected?</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>No comment.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>No comment.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>No comment.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>I agree that it is necessary to apply the same CDD standards pre and post licensing. However, it is difficult to specify an appropriate timeframe as it depends on the size of the DTSP's pre-licensing customer base and the gap between its CDD measures pre and post licensing and the time required to close the gap. In FSM-N27, paragraph 6.54, the time period to complete CDD for Pre-License customer is stated as "to be determined by the Authority". It would be good if MAS can exercise flexibility in determining a suitable period for each license applicant on a case-by-case basis.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>No comment.</p>



S/N	Respondent	Responses from respondent
		<p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>No comment.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>No comment.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>No comment.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>No comment.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>No comment.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>No comment.</p> <p>Question 13.</p>



S/N	Respondent	Responses from respondent
		<p>Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>No comment.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>No comment.</p>
12	Respondent C	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>It is noted that under the Payment Services Regulation and corresponding Guidelines, the pro-ration of annual licence fee(s) is on ALL licences (existing and newly approved) held by the licensee (refer to example in Appendix 4 of Guidelines on Licensing for Payment Service Providers). It is felt that such a methodology results in double payment of annual licence fee(s) for existing licence(s).</p> <p>The drafting of the draft Regulation, which uses the term “licence”, does not seem to follow the same formula as the existing Guidelines.</p> <p>It would be good to confirm that the intent of the Schedule Fees pro-ration is to apply pro-ration only on the DTSP licence, and not on the cumulative licences held by the licensee.</p> <p>If so, the existing pro-ration calculation should be aligned to make fees payable fairer.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>No feedback.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>No feedback.</p>



S/N	Respondent	Responses from respondent
		<p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>No feedback.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>It is agreed that CDD measures must be performed on all existing customers. However, some licensees may have amassed a large clientele prior to obtaining its DTSP licence.</p> <p>It is suggested that discretion be given for a licensee to approach the CDD using a risk-based basis, provided the licensee had established a robust risk management framework. The “reasonable time period” could be stratified in accordance to the risk classification of its customers. E.g. customers categorised as high risk be completed in 6 months; medium - 1 year; and low risk - 3 years or on a sample basis. Justification for the risk-based approach has to be properly documented and approved by the Board of Directors or delegated Board Risk Management Committee.</p> <p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>No feedback.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>No feedback.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>No feedback.</p> <p>Question 9.</p>



S/N	Respondent	Responses from respondent
		<p>Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>No feedback.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>From the reading of para 5.9 of the Consultation Paper together with para 5.10, it seems to allow the value transfer to proceed even if there are lack of the required value transfer originator or value transfer beneficiary information. It would be appreciated if MAS could confirm that this is the case, and the lack of such information does not prohibit the value transfer.</p> <p>In relation to para 6.58 of FSM-N27 - screening value transfer beneficiary - it is noted that information specified in 14.4(a) - (d) does not include sufficient details to facilitate the disposition of a name match. Therefore, it might be challenging to perform such screening without delaying the transaction. If a name match is encountered, a licensee will have to request for more identifying information of the beneficiary in order to approve/ decline the transaction. This may cause friction and/ or lead to tipping-off the parties.</p> <p>It is proposed that the ordering institution be responsible for screening the originator, while the beneficiary institution screens the beneficiary, who in all likelihood is already its customer.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>No feedback.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p> <p>No feedback.</p>



S/N	Respondent	Responses from respondent
		<p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>No feedback.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>No feedback.</p>
13	Respondent D	<p>Question 1. Licensing processes, and fees. MAS seeks comments on the processes and timelines for licence application and lapsing, as well as the fee structures and the quantum of the fees proposed.</p> <p>\$5++.</p> <p>Question 2. Minimum financial requirements. MAS seeks comments on the quantum and components of the proposed minimum financial requirements.</p> <p>800.</p> <p>Question 3. Duties of the CEO, directors and partners of the licensee, and audit requirements. MAS seeks comments on the proposed duties of the CEO, directors, and partners of the licensee. MAS also seeks comments on the audit requirements.</p> <p>No comments.</p> <p>Question 4. General comments. If you have comments on the measures proposed in parts 5-8, please set them out in response to this question.</p> <p>Nil.</p> <p>Question 5. Existing Customers. MAS seeks comments on the requirements for existing customers that were onboarded by the licensee prior to obtaining its licence. (Please refer to paragraph 6.54 and 6.55 of the draft FSM Notice).</p> <p>Nil.</p>



S/N	Respondent	Responses from respondent
		<p>Question 6. Reliance on Third Party. MAS seeks comments on whether third party reliance is appropriate for the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>Sorry for the way we do.</p> <p>Question 7. Reliance on Third Party. MAS seeks comments on the proposed amendments to the other AML/CFT notices.</p> <p>Ty.</p> <p>Question 8. Correspondent Account Services. MAS seeks comments on whether the proposed requirements for Correspondent Account Services set out in paragraph 5.6 would be applicable to the sector. (Please refer to paragraph 12 of the draft FSM Notice).</p> <p>I already mailed to opt out.</p> <p>Question 9. Bearer Negotiable Instruments and Cash Payouts. MAS seeks comments on the proposal in paragraph 5.7 to apply the prohibition of issuance of bearer negotiable instruments and restriction on cash payout to licensees. (Please refer to paragraph 10 of the draft FSM Notice).</p> <p>No payment is given at all.</p> <p>Question 10. Value Transfer Requirements for DT Services. MAS seeks comments on the type of information that accompanies or relates to value transfers that would be relevant for law enforcement purposes, and the type of records that should be kept. Please also provide examples of how this requirement could be operationalised in practice, including industry-wide initiatives. (Please refer to paragraph 14 of the draft FSM Notice).</p> <p>We hope I do Ur things properly.</p> <p>Question 11. Reporting requirements. MAS seeks comments on the draft FSM-N28 and FSM-N29.</p> <p>No comments.</p> <p>Question 12. Technology risk management and cyber hygiene requirements. MAS seeks comments on the draft FSM-N30 and FSM-N31.</p>



S/N	Respondent	Responses from respondent
		<p>No comments.</p> <p>Question 13. Requirements on conduct, disclosure and communications. MAS seeks comments on the draft FSM-N32 and FSM-N33. In particular, please let us have your views on the requirements relating to the proposed operating days and hours (under FSM-N32). In addition, MAS seeks comments on the disclosure requirements as well as requirements concerning false or misleading scope of regulation.</p> <p>No comments.</p> <p>Question 14. Guidelines. MAS seeks comments on the application of the guidelines referred to paragraphs 8.1 and 8.2 to licensees.</p> <p>Improve.</p>