VIRTUAL ASSET GUIDANCE 2026 (Version 1.0)

Table of Contents

INTRODUCTION

1) This Guidance is issued by the Gelephu Financial Services Office ("GFSO") under section 15(1) of the Financial Services Act 2025 ("FSA") in respect of the Virtual Asset ("VA") regime in Gelephu Mindfulness City ("GMC"). It should be read in conjunction with the FSA and the relevant Rulebooks.

2) This Guidance is primarily applicable to the following Persons:

   a) an Applicant for a Financial Services Licence ("FSL") to carry on a VA Regulated Activity in or from GMC; or

   b) a Licensed Firm conducting a VA Regulated Activity in or from GMC.

3) This Guidance sets out the GFSO approach to the regulation of the use of Virtual Assets in GMC. This Guidance, together with the FSA and GFSO Rulebooks governing the use of Virtual Assets, is collectively referred to as the "Virtual Asset Framework".

4) This Guidance is not an exhaustive source of the GFSO's policy on the exercise of its regulatory functions and powers. The GFSO is not bound by the requirements set out in this Guidance and may:

   a) impose additional requirements to address any specific risks posed in relation to the use of Virtual Assets; and

   b) waive or modify any of the Rules relevant to the Virtual Asset Framework, at its discretion, where appropriate.

5) Unless otherwise defined or the context otherwise requires, the terms contained in this Guidance have the same meaning as defined in the FSA and the Glossary Rulebook ("GLO").

6) The term "Licensed Firm" is generally used in this Guidance to refer to a Licensed Firm in GMC permitted to carry on a VA Regulated Activity or a Licensed Exchange permitted to operate a Multilateral Trading Facility (in relation to Virtual Assets). Where the context so requires (e.g., in relation to AML obligations), the term "Licensed Firm" should be read as including a Licensed Firm conducting Regulated Activities other than VA Regulated Activities.

7) For more details on the licensing process in GMC, please contact the GFSO at gfso@gmc.bt.

BACKGROUND

8) This Guidance focuses on the GFSO regulatory treatment of Virtual Assets, and the financial services activities that can be conducted in relation to Virtual Assets within GMC. For the purposes of the Virtual Asset Framework, "Virtual Assets" is defined in the FSA as follows:

"Virtual Asset" means a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. A Virtual Asset is -

a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Virtual Asset;

b) distinguished from Fiat Currency and E-money; and

c) not a Specified Investment, Fiat-Referenced Token or Spot Commodity."

9) The following table sets out the GFSO regulatory approach in relation to different types of digital assets.

Digital Asset Types	**GFSO Regulatory Treatment**
Virtual Assets	Refers to non-fiat virtual currencies (such as BTC, ETH, BNB, SOL etc). Firms conducting regulative activities in GMC with respect to spot Virtual Assets are required to apply to the GFSO for an FSL.
Fiat-Referenced Tokens	Fiat-Referenced Tokens ("FRTs") are a category of stablecoin backed by high quality, liquid assets denominated in the same currency as the FRT. Issuing a FRT is a distinct Regulated Activity in GMC and requires an FSL.
Digital Securities	Refers to digital assets with Security characteristics (including 'tokenised' offerings of Securities). Financial services activities in relation to Security Tokens – e.g. the offering of, dealing in, providing custody of, or advising on Security Tokens are regulated as Security instruments under FSA.
Derivatives/Funds	Derivatives over regulated Digital Assets, and Collective Investment Funds investing in regulated Digital Assets, are regulated as Derivatives and Units in a Fund under FSA. Offering such products requires an FSL, but are regulated as non-spot products.

KEY FEATURES OF THE VIRTUAL ASSET FRAMEWORK

VA Regulated Activities

10) The principal Rules for Licensed Firms conducting a VA Regulated Activity are set out in Chapter 17 of the Conduct of Business Rulebook ("COBS"). COBS Rule 17.1.2 operates as a 'sign-post' Rule designed to draw the attention of Licensed Firms conducting a VA Regulated

Activity to the fact that they must comply with all Rules applicable to Licensed Firms, including:

a) all other relevant chapters of COBS;

b) the General Rulebook ("GEN");

c) the Anti-Money Laundering and Sanctions Rulebook ("AML"); and

d) the Code of Market Conduct ("CMC").

11) The table below sets out the main risk areas, and the related mitigations for each of these risk areas, under the Virtual Asset Framework.

RISK		MITIGANT
1.	AML/CFT/ SANCTIONS/TAX	The AML Rulebook applies in full to all Licensed Firms.
2.	CONSUMER PROTECTION	All material risks associated with Virtual Asset products, services and activities must be appropriately disclosed, and monitored and updated on an ongoing basis.
3.	TECHNOLOGY GOVERNANCE	Systems and controls must be in place in relation to: ● Virtual Asset wallets; ● Private keys; ● Origin and destination of Virtual Asset funds; ● Security; and ● Risk management, business continuity and systems recovery.
4.	'EXCHANGE-TYPE' ACTIVITIES	Multilateral Trading Facilities (MTFs) using Virtual Assets are required to have in place, among other things, the following: ● Market surveillance; ● Fair and orderly trading; ● Market abuse prevention; ● Settlement processes; ● Transaction recording; ● A rulebook(s); ● Transparency and public disclosure mechanisms; and ● Exchange-like operational systems and controls.

5.	CUSTODY	Virtual Asset Custodians are subject to Chapter 15 (read together with Rule 17.8) and Chapter 16 of COBS. Frequent reconciliations and reporting of Virtual Assets, as well as appropriate internal controls to safeguard them, are required.

Combination of Regulated Activities

12) Applicants approved by the GFSO as a Licensed Firm and permitted to conduct a VA Regulated Activity will be granted an FSL for the relevant Regulated Activity. An Applicant seeking to conduct activities in relation to non-Virtual Assets (i.e. Specified Investments / Financial Instruments), in addition to Virtual Assets, will need to apply to the GFSO to be able to do so, and will need to comply with the GFSO's requirements in relation to those Specified Investments / Financial Instruments.

GFSO powers in respect of Virtual Assets

13) Licensed Firms conducting VA Regulated Activities should note that the GFSO has broad powers under section 5A and 5B of the FSA. For example, the GFSO has powers to require a Licensed Firm to either take such action as the GFSO may specify, or cease the conduct of a Regulated Activity in respect of a Virtual Asset, for such period of time as the GFSO deems s appropriate.

REQUIREMENTS FOR LICENSED FIRMS ENGAGED IN REGULATED ACTIVITIES IN RELATION TO VIRTUAL ASSETS

Conducting a Regulated Activity in relation to Virtual Assets

14) Chapter 17 of COBS applies to all Licensed Firms conducting a VA Regulated Activity, requiring compliance with all requirements set out in COBS Rules 17.1 to 17.6. Licensed Firms that are Operating a Multilateral Trading Facility or Providing Custody in relation to Virtual Assets are also required to comply with the additional requirements set out in COBS Rules 17.7 and 17.8 respectively.

Accepted Virtual Assets

15) COBS Rule 17.2.1 provides that a Licensed Firm conducting any VA Regulated Activity shall not conduct such Regulated Activity with a Virtual Asset which is not an Accepted Virtual Asset. A Licensed Firm is obliged to assess each Virtual Asset it proposes to use against the criteria outlined in COBS Rule 17.2.2 to determine whether that Virtual Asset meets the GFSO's requirements for an Accepted Virtual Asset. It is also required to notify the GFSO upon completion of that assessment no later than five Business Days prior to using the Virtual Asset.

16) Prior to assessing a particular digital asset against the criteria outlined in COBS Rule 17.2.2, a Licensed Firm must carefully consider the definition of 'Virtual Asset' and confirm that the relevant asset satisfies that definition.

Guidance on governance arrangements in respect of assessing Virtual Assets

17) For the purposes of making and submitting an assessment under COBS Rule 17.2, a Licensed Firm should ensure that it has suitable and robust governance framework in place to effectively assess, and continuously monitor, that the Virtual Assets recognised, or proposed to be recognised, as Accepted Virtual Assets by the Licensed Firm comply with the requirements set out in COBS Rule 17.2. The GFSO expects that a Licensed Firm's governance framework will be proportionate to its nature, scale and complexity and will be properly documented and adhered to. For example, larger Licensed Firms should consider establishing a dedicated committee and associated process, while smaller Licensed Firms may consider it appropriate to be conducted through its relevant key functions (e.g. compliance, risk management, information technology, operations etc). Such governance framework should clearly define responsibilities for decisions relating to the change in use of Accepted Virtual Assets by a Licensed Firm, including adding, suspending/halting or removing a Virtual Asset from being offered as part of a VA Regulated Activity.

18) Licensed Firms should engage with the GFSO for the purpose of implementation of these governance arrangements. These arrangements should also be reviewed periodically by the relevant key functions within the Licensed Firm, with such reviews and findings properly documented and available for review by the GFSO, as required.

19) Licensed Firms should establish and maintain suitable record keeping arrangements, including comprehensive documentation and accurate records related to both initial and ongoing Virtual Asset assessments, including supporting evidence, relevant notifications submitted to the GFSO, and client communications and disclosures.

Accepted Virtual Asset assessment criteria

20) A Virtual Asset that meets the GFSO's requirements will constitute an Accepted Virtual Asset for that Licensed Firm only. COBS Rule 17.2.2 states that, for the purpose of determining whether a Virtual Asset meets the requirements of being an Accepted Virtual Asset, a Licensed Firm must adequately assess the following criteria:

a) Traceability/monitoring: whether Licensed Firms are able to demonstrate the origin and destination of the specific Virtual Asset, if the Virtual Asset enables the identification of counterparties to each transaction, and if on-chain transactions in the Virtual Asset can be adequately monitored;

b) Security: whether the Virtual Asset is able to withstand, adapt, respond to, and improve on its specific risks and vulnerabilities, including relevant factors and risks relating to its use,

including testing, maturity, and ability to allow the appropriate safeguarding of secure private keys;

c) Market profile: the duration that the Virtual Asset has been in existence, the sufficiency, depth and breadth of market demand, the proportion of the Virtual Asset that is in circulation, the controls/processes to manage potential volatility of such Virtual Asset and any sanction and adverse media in respect of the parties associated with the Virtual Asset, including founders, contributors, foundation members, investors and key decision-makers. This extends to establishing whether there is any association of the Virtual Asset with illegal activities or any serious concerns that its use may circumvent sanctions/restrictions;

d) Exchange connectivity: whether there are exchanges that support the Virtual Asset; the jurisdictions of these exchanges and whether such exchanges are suitably regulated;

e) DLT infrastructure and ecosystem: whether there are issues relating to the underlying blockchain's consensus mechanism, its security and/or usability of the DLT used for the purposes of the Virtual Asset; including whether the Virtual Asset leverages an existing DLT for network and other synergies, and, in the case of a new DLT, whether the new DLT has been demonstrably stress tested;

f) Innovation / efficiency: whether the Virtual Asset demonstrates utility by, for instance, helping to solve a fundamental problem, addressing an unmet market need or creating value for network participants; and

g) Practical application / functionality: whether the Virtual Asset possesses quantifiable functionality.

21) In preparing an assessment for a Virtual Asset, the GFSO expects Licensed Firms to conduct a risk-based, comprehensive, and objective assessment. This assessment should include the criteria outlined in COBS Rule 17.2.2 as elaborated upon in paragraph 33 below.

22) A Licensed Firm should consider the relative importance of each criterion taking into account all relevant considerations, including the Licensed Firm's Regulated Activities and the nature of the Virtual Asset being assessed.

Process for notifying the GFSO regarding new Virtual Assets

23) ALicensed Firms seeking to use a new Virtual Asset should arrange a discussion with the GFSO prior to offering the Virtual Asset.

Continuous monitoring

24) A Licensed Firm conducting a VA Regulated Activity in relation to an Accepted Virtual Asset must continuously monitor such Accepted Virtual Asset to ensure that it continues to satisfy the criteria specified in COBS Rule 17.2.2. The GFSO expects that a Licensed Firm's processes will include clear policies and procedures to address changes, whether significant or not, which

may affect how a particular Accepted Virtual Asset satisfies the criteria specified in COBS 17.2.2. These processes should encompass reporting to the GFSO where appropriate (noting applicable reporting obligations under GEN and COBS) and any action to be taken by the Licensed Firm.

Capital Requirements

25) The table below sets out the capital requirements for Licensed Firms carrying out VA Regulated Activities:

Regulated Activity	**Examples of Such VA Business Models**	**Capital Requirement**
Prudential Category 2 Dealing in Investments as unmatched Principal	A firm that sells VA products such as options, with the firm taking the other side of the position as principal and taking the risk onto its books.	US$200,000 or 6 months operational expenses, whichever is higher.
Prudential Category 3A Dealing in Investments as Matched Principal Dealing in Investments as Agent	Matched principal: A firm that sells or buys VAs with clients, but immediately squares off its position by buying/selling the same with another firm. Agent: A firm that is a broker acting solely as an agent that helps clients place VA trades with another firm.	US$200,000 or 6 months operational expenses, whichever is higher.
Prudential Category 3C Providing Custody Providing Money Service Managing Assets	Providing Custody: A firm that custodizes the crypto of clients by holding the private keys. Providing Money Services: A firm that provides VA remittances and/or conversions involving VAs. Managing Assets:A firm that takes clients' funds to invest into crypto (but does not pool clients' funds).	US$200,000 or 6 months operational expenses, whichever is higher.

Regulated Activity	Examples of Such VA Business Models	Capital Requirement
Prudential Category 4 Arranging Deals in Investments Advising on Investments or Credit Arranging Custody	Arranging Deals in Investments: A firm that does corporate finance-type work by helping link up investors with crypto projects seeking investments. Advising on Investments or Credit: A firm that only provides advice to clients on crypto investments or crypto credit products, but does not execute or manage the investment. Arranging Custody: Firm A that represents to clients that it does not do the actual custody of VA, but will help clients contract with a third party Firm B that is either part of the same group or pays Firm A a commission for the introduction.	US$10,000 or 6 months operational expenses, whichever is higher. This is because these regulated activities are lower risk, and the firm does not handle clients' funds.
Prudential Category 4 Operating an MTF	A crypto exchange	US$500,000 or 12 months operational expenses, whichever is higher

26) Pursuant to these Rules, regulatory capital must be held by a Licensed Firm in fiat form. Operational expenses calculated by firms under MIR Rule 3.2 should be in accordance with the International Financial Reporting Standards (IFRS).

27) Operational expenses, as set out in MIR Rule 3.2.1, broadly includes all of the overhead, non-discretionary costs (variable and exceptional items can be excluded) incurred (or forecast to be incurred) by a Licensed Firm in its operations over the course of a 12-month period. Technology-related operational expenses, such as the use of IT servers and technology platforms, storage and usage of IT equipment and technology services required for the overall operability of the Licensed Firm's platform, are to be included. Development costs, such as research and intellectual property patenting can be excluded.

28) The GFSO may impose additional capital requirements on a particular Licensed Firm where it considers that its regulatory capital requirement is insufficient to adequately address all relevant risks.

Anti-Money Laundering and Countering Financing of Terrorism

29) The use of Virtual Assets raises significant regulatory concerns for regulatory authorities and law enforcement agencies worldwide, particularly in relation to Money Laundering ("ML") and Terrorism Financing ("TF"). International bodies, such as the International Monetary Fund ("IMF"), the Financial Action Task Force ("FATF"), the Bank for International Settlements

("BIS") and the International Organisation for Securities Commissions ("IOSCO"), have issued different Digital Asset (including Virtual Asset and ICO) warnings to investors and market participants advising of the significant risks, including ML and TF risks, and the possibility of Digital Assets being used for wider illegal purposes.

30) FATF has identified certain key risks associated with Virtual Assets, which include the following:

a) Digital Assets (including, in particular, Virtual Assets) may operate in an anonymous or pseudo-anonymous manner. Virtual Assets can be traded online, are generally characterised by non-face-to-face Client relationships, and may permit (pseudo-) anonymous funding and transfers;

b) The global reach of Virtual Assets increases the potential for ML/TF risks. Virtual Asset systems can be accessed via the Internet (including via mobile phones), and can be used to make cross-border payments and fund transfers;

c) Virtual Asset platforms commonly rely on complex infrastructures utilising several entities, often spanning multiple countries, to transfer funds or execute payments. This segmentation of services means that responsibility for ML/TF compliance and supervision/enforcement may be unclear. Moreover, Client and transaction records may be held by different entities, in different jurisdictions, making it more difficult for regulators and law enforcement agencies to access them. These issues are exacerbated by the rapidly evolving nature of 'decentralised' technologies used by Virtual Asset businesses, including the changing number and types/roles of participants providing services in the Virtual Asset ecosystem; and

d) Components of the Virtual Asset system may be located in jurisdictions that do not have adequate ML/TF controls.

31) Taking into account Virtual Asset ML and TF risks, the importance of meeting global transparency and beneficial ownership standards, and the need to have proper mechanism to exchange information with other regulators and counterparties, the GFSO requires that its AML Rules apply to all Licensed Firms, including those engaged in conducting a Regulated Activity in relation to Virtual Assets.

Key considerations for AML/CFT compliance

32) When considering the FATF Recommendations, in combination with the application of the AML Rules, the GFSO notes the following key principles that a Licensed Firm conducting a Regulated Activity in relation to Virtual Assets should consider:

Principle 1: Risk-Based Approach

33) FATF expects countries, regulators, financial institutions and other concerned parties to adopt a 'Risk-Based Approach' ("RBA"). Licensed Firms are expected to understand the risks

associated with their activities and allocate proper resources to mitigate those risks. A RBA can only be achieved if it is embedded into the compliance culture of the Licensed Firm, which enables the Licensed Firm to make decisions and allocate appropriate resources in the most efficient and effective way.

34) Licensed Firms should, on a periodic basis, carry out a proper risk-based assessment of their processes and activities. In order to implement the RBA, Licensed Firms are expected to have processes in place to identify, assess, monitor, manage and mitigate ML risks. The general principle is that in circumstances where there are higher risks of ML, Licensed Firms are required to implement enhanced measures to manage and mitigate those risks.

Principle 2: Business Risk Assessment

35) Chapter 6 of the AML Rules requires Relevant Persons to take appropriate steps to identify and assess the ML risks to which their businesses are exposed, taking into consideration the nature, size and complexity of their activities. When identifying and assessing these risks, several factors should be considered, including an assessment of the use of new technologies. Importantly, in the context of Virtual Assets, FATF Recommendation (15) states that: "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks."

36) Another aspect of assessing the business risk relevant to Licensed Firms is gaining familiarity with the characteristics and terminology of the Virtual Asset industry. Additionally, Licensed Firms, and their management and staff, should be aware of the possible misuse of Virtual Assets in criminal activities, as well as the technical and complicated nature of Virtual Assets (and the platforms they operate on).

37) When making its assessment, a Licensed Firm must give consideration to all business risks. For example, while an issue may be identified in relation to cyber security (e.g., when dealing with wallets or using cloud computing to store data – being a 'technology' risk), the GFSO expects Licensed Firms to consider these risks from all perspectives to establish whether the risk triggers other issues for consideration (including ML/TF risks, technology governance and consumer protection). A Licensed Firm must then use the identified risks to develop and maintain its AML/CTF policies, procedures, systems and controls and take all reasonable steps to eliminate or manage such risks.

Principle 3: Customer Risk Assessment and Customer Due Diligence

38) The GFSO expects all Licensed Firms to have fully compliant Client on-boarding processes. Virtual Assets have been criticised by regulatory bodies globally due to their

(pseudo-)anonymity features, which makes tracking Client records and transactions more challenging for compliance officers and money laundering reporting officers.

39) Customer Risk Assessment and 'Customer Due Diligence' ("CDD") policies and procedures are required to be implemented by all Licensed Firms. Licensed Firms should have a process to assess and rate all their Clients according to that Client's risk profile (and taking into consideration the Licensed Firms' RBA). This risk-based assessment is required to be undertaken for each Client prior to transacting any business on behalf of the Client. Licensed Firms must undertake CDD for each Client and comply in full with Chapter 8 of the AML Rules noting that the GFSO does not consider it appropriate for Licensed Firms to use simplified CDD when conducting a Regulated Activity in relation to Virtual Assets, largely due to issues surrounding the (pseudo-) anonymity of Clients and transactions associated with Virtual Assets.

40) In the case of non-face-to-face on-boarding and ongoing due diligence of Clients who are natural persons, the GFSO expects that a Licensed Firm will develop appropriate policies to ensure that the Client's identity is duly verified in accordance with all applicable Laws and Rules. This may include obtaining a "selfie" or by conducting a "liveness test". Irrespective of the method employed, it should validate that the individual being on-boarded is present during the on-boarding process, matches the individual in the identity documentation, and that the ID presented is valid and authentic. It should also include obtaining and authenticating a valid form of the Client's facial ID, which should be either the Client's passport with all applicable details clear and, or the original version (front and back) of an official government issued document, such as a national ID or driver's license.

41) The GFSO understands that Licensed Firms may need to use new technology to improve Client on-boarding processes for the purpose of assessing and managing ML and TF risks. For example, in order for Licensed Firms to conduct non-face-to-face on-boarding they will need to implement facial recognition software to validate the "selfie" against the other uploaded documentation, or other suitable biometric technology.

42) The GFSO further understands that the proper use of such technologies (e.g., fingerprinting, retinal/eye scans, use of real-time video conference facilities to enable facial recognition) can assist with mitigation of the ML/TF risks associated with the use of Virtual Assets. Technological features, such as secure digital signatures that allow the verification of a Client's identity through a signed document, may also be acceptable to the GFSO. In all cases, a Licensed Firm should ensure that the use of these technologies will not lead to a simplified process where the required Customer Risk Assessment and CDD requirements are not appropriately undertaken by a Licensed Firm.

43) The GFSO recommends that Licensed Firms obtain a signed self-certification from their Clients identifying the details of all passports issued and held in their name(s). Licensed Firms may also use this as an opportunity to capture all tax related details in order to meet their international tax

reporting obligations. Self-certification should not prevent Licensed Firms from conducting proper CDD.

Principle 4: Governance, Systems and Controls

44) Licensed Firms are required to implement an appropriate governance structure, especially in relation to Information Technology governance, and provide for the development and maintenance of all necessary systems and controls to ensure appropriate ML and TF compliance.

45) The GFSO expects that Licensed Firms may seek to utilise (their own or third-party) technologies and solutions to meet their regulatory obligations (e.g., customer risk assessment, detection of fraud, and transaction identification, monitoring and reporting) and risk management requirements (e.g., margin limits, large exposure monitoring).

46) The GFSO expects Licensed Firms to develop, implement and maintain effective transactional monitoring systems to determine the origin of a Virtual Asset and to monitor its destination, and to apply strong "know your transaction" measures which enable Licensed Firms to have complete granular data centric information about the transactions done by a Client.

47) The GFSO expects Licensed Firms to act responsibly and always be vigilant in ensuring that their activities are not subject to any misuse by participants transacting with Virtual Assets that may have been tainted in any way from an illegal activity. The GFSO expects that a Licensed Firm's internal processes establish the types of 'indicators' or activities that could be used to identify when Accepted Virtual Assets may have been used in an illegal manner. A Licensed Firm should have a process for the management of when such 'indicators' (for example, certain Client or use of "mixer" and "tumbler" services) are triggered.

48) While the GFSO cannot recommend particular vendors or providers, all technology solutions must be fit for purpose and Licensed Firms should consider using those with an established track record and undertake their own due diligence/risk assessment to ensure competency and capability. The GFSO recognises that many of the (technology) solutions appropriate for mitigating Virtual Asset risks are continuing to be developed within the Virtual Asset industry itself.

49) Licensed Firms must appoint a Money Laundering Reporting Officer ("MLRO") who will be responsible for the implementation and oversight of the Licensed Firm's compliance with the AML Rules. Consistent with the GFSO's expectation in relation to all other Licensed Firms, an MLRO should have an appropriate level of seniority and independence to be effective in the role.

Principle 5: Suspicious Activity Reporting obligations

50) Licensed Firms should familiarise themselves with their reporting obligations under the AML Rules, in particular in relation to the reporting of suspicious activities/transactions.

51) Licensed Firms are required to establish sophisticated transaction monitoring systems to detect possible ML and TF activities. Systems should also be implemented to effectively identify any attempt to breach domestic and international sanctions. Such systems may rely on new technological solutions (including monitoring algorithms or Artificial Intelligence ("AI")).

52) Where a Licensed Firm has determined that it wishes to file a Suspicious Activity Report ("STR"), it should file these reports with the GFSO.

Principle 6: Record keeping

53) As proper documentation is one of the main pillars of ensuring AML/CFT compliance, Licensed Firms are required to have policies and procedures in place to ensure proper record keeping practices. It is expected that a Licensed Firm will maintain up to date records in accordance with the CDD obligations applicable to it and be prepared to provide the records upon request from the GFSO.

54) The GFSO understands that the transaction recording of many Virtual Asset transactions is linked to, or based on, DLT. This requires a Licensed Firm to implement specific arrangements to ensure that, at a minimum, the Licensed Firm and the GFSO have access to all relevant information as necessary. A Licensed Firm may use a distributed ledger to store its data, provided it is able to provide this data, in an easily accessible format, to the GFSO when required.

55) The GFSO views Virtual Asset activities that are linked to cash transactions as posing higher ML and TF risks, due to the source of funding being significantly more difficult to determine. Licensed Firms wishing to conduct cash transactions will be required to implement enhanced controls to mitigate the inherent risks of such transactions. Such controls may include, among other things, setting appropriate limits on cash deposits (e.g., daily, monthly, yearly limits), a prohibition on receiving cash directly, prohibitions on the receipt of cash other than from bank accounts, and prohibitions on receiving funds from third parties. In all cases, Licensed Firms will need to clearly demonstrate to the GFSO how their controls suitably mitigate the risks of cash transactions within their operations. Considering the wider consumer protection implications, the GFSO also considers it unlikely to be appropriate for Licensed Firms to accept deposits by way of credit card or credit facilities/credit lines.

56) GFSO expects all Licensed Firms to exercise due care, to the utmost extent possible, in their day-to-day operations and when dealing with Clients or potential Clients. A Licensed Firm's activities are expected to comply with the AML Rules, ensuring that their activities do not pose a regulatory risk or reputational damage to GMC.

Technology Governance and Controls

57) Historically, Virtual Asset business failures have often arisen as a result of the lack of adequate technology-related procedures, including, for example, lack of security measures, systems development methodologies, limited system penetration testing for operating a robust business

and lack of technical leadership and management. The GFSO has therefore included this specific guidance regarding expected controls and processes to help mitigate these issues.

58) GEN Rule 3.3 requires an Licensed Firm to establish systems and controls to ensure its affairs are managed effectively and responsibly, and to ensure such systems and controls are subject to continuous monitoring and review. COBS Rule 17.5 sets out additional requirements for appropriate technology governance and controls specific to Licensed Firms, with a focus on:

a) Virtual Asset Wallets;

b) Private and Public Keys;

c) Origin and destination of Virtual Asset funds;

d) Security; and

e) Risk Management.

59) When complying with GEN Rule 3.3 and COBS Rule 17.5, Licensed Firms should have due regard to the following key areas from a technology perspective:

a) Careful maintenance and development of systems and architecture (e.g., code version control, implementation of updates, issue resolution, and regular internal and third party testing);

b) Security measures and procedures for the safe storage and transmission of data;

c) Business continuity and Client engagement planning in the event of both planned and unplanned system outages;

d) Processes and procedures specifying management of personnel and decision-making by qualified staff; and

e) Procedures for the creation and management of services, interfaces and channels provided by or to third parties (as recipients and providers of data or services).

Maintenance and development of systems

60) Licensed Firms are expected to have a well-defined, documented and deliberate approach for the implementation and upgrade of systems and software.

61) Licensed Firms should also have well-established policies and procedures for the regular and thorough testing of any system currently implemented or being considered for use (e.g., upgrades to a matching engine or opening of a new Application Programming Interface (“API”) internally or with a third party).

62) The updated system should be tested for technical, operational and security vulnerabilities including but not limited to functional, penetration and stress testing. The outcome of the testing

should be well structured and documented and signed off by the responsible (technology-focused) executives of the Licensed Firm.

63) All changes made to the codebase in use are to be tracked and recorded, with a clear audit trail for appropriate internal checks and sign-off. The use of a version control system which allows for the accurate timestamping and identification of the user responsible for relevant changes should be considered.

64) Licensed Firms should maintain a clear and comprehensive audit trail for system issues internally, including security issues and those with third parties, their resolution and implementation of fixes.

65) Licensed Firms should conduct at least annual third-party verification/audit of core systems being used (including, if relevant, verification / audit of custody arrangements and verification of the amount of their purported holdings of Virtual Assets and Client Money). MTFs using Virtual Assets and Virtual Asset Custodians should have an annual review of their infrastructure undertaken by reputable third-party cyber security consultants, producing a list of recommendations and areas of concern.

Security measures and procedures

66) Licensed Firms should have measures and procedures in place which comply with network security industry best practices (e.g., the implementation of firewalls, strong passwords, password management procedures, multifactor authentication and encryption of data in transit and at rest).

67) Updates and patches to all systems, particularly security systems, should be performed as soon as safely feasible after such updates and patches have been released, whether these systems have been developed internally or developed by a third-party.

68) An Licensed Firm's IT infrastructures (particularly for MTFs using Virtual Assets and Virtual Asset Custodians) are expected to provide strong layered security and seek the elimination of "single points of failure". IT infrastructure security policies are required to be maintained, describing in particular how strong layered security is provided and how "single points of failure" are eliminated. This includes, but should not be limited to, systems and procedures to limit the access of a single user to the use of private and confidential information of Clients.

69) IT infrastructures should be strong enough to resist, without significant loss to Clients, a number of scenarios, including but not limited to: accidental destruction or breach of data, collusion or leakage of information by employees/former employees, successful hack of a cryptographic and hardware security module or server, or access by hackers of any single set of encryption/decryption keys that could result in a complete system breach.

70) Licensed Firms should have in place policies and procedures that address information security for all personnel. The security policy should set the security tone for the whole entity and inform personnel what is expected of them. All personnel should be aware of the sensitivity of

data and their responsibilities for protecting it. To mitigate "key person risk", Licensed Firms are to ensure that there is no single individual that holds privileged or sensitive information that is critical to the operation of the Licensed Firm.

71) The strong encryption of data, both at rest and in transit, should be included in the security policy. In particular, encryption and decryption of Virtual Asset private keys should utilise strong encryption protocols and algorithms that have broad acceptance with cyber security professionals. Critical cryptographic functions such as encryption, decryption, generation of private keys, and the use of digital signatures should only be performed within cryptographic modules complying with the highest, and internationally recognised, applicable security standards.

72) All security incidents and breaches should be logged and documented in detail as soon as practicable and the resolution and implementation details should subsequently be added to the log.

73) The use of open source software should be governed by clear, well documented and transparent rules and procedures governing the software's stability, security and fitness for purpose. Any open-source software, whether it is a compiled distribution or code, should be thoroughly tested for security and operational vulnerabilities. This testing should be signed off by the responsible executives of the Licensed Firm before being used for the processing or storing of operational and Client information.

74) All APIs that are internal or external facing should be secured by strict access management procedures and systems, including encryption of the information (e.g., SSL certificates). All API access activity should be logged and scanned for security breaches on an ongoing basis.

75) All access management and credential changes (for employees, third-party service providers and Clients) should be governed and monitored by strict and well documented rules and procedures. This should include, but not be limited to, enforcing strong passwords and the monitoring of IP geo-location, use of VPN, TOR or unencrypted web connections.

Cryptographic Keys and wallet storage

76) The ability to send and receive Virtual Assets by recording new transactions on a distributed ledger is usually dependent on cryptographic keys – a public key and one or more private keys. The public key allows other users on a distributed ledger to send Virtual Assets to an address associated with that public key. The private key(s) provides full control of the Virtual Assets associated with the public key. As such, Licensed Firms need to have robust procedures and protective measures to ensure the secure offline generation, storage, backup and destruction of both public and private keys for their own wallet operations and where they offer wallet services to Clients.

77) Whether private keys are held on network attached devices or devices that are offline, Licensed Firms must have policies and procedures to ensure that they are not compromised by malicious actors.

Password protection and encryption

78) Licensed Firms should consider using wallets that require multiple private keys or combining the distributed parts of a private key to authorise transactions. Where this is not practical or feasible, a similar mechanism or procedure should be in place (e.g., a multi-user authentication prior to authorising transfers from wallets).

79) Licensed Firms must have policies and procedures in place that set out actions and responsibilities in the event of a breach of private and public keys, as well as Client user access credentials.

Origin and destination of Virtual Asset funds

80) Virtual Asset transactions between public addresses take place on public DLT. Although it is normally possible to identify the public addresses of the parties to a transaction, it is often very difficult to establish the owner (whether natural or legal) of these addresses. This makes Virtual Assets attractive to money launderers, terrorist financers and other criminals.

81) The US Office of Foreign Asset Control (OFAC) has issued a statement requiring wallet addresses known to belong to individuals listed on the Specially Designated Nationals and Blocked Persons sanctions ("SDN") list to be reported. Further information is available on the OFAC website. Additionally, there are companies collecting "tainted" wallet addresses that have been used in hacks, "dark web" transactions and other criminal activities.

82) A Licensed Firm must have clear policies and procedures, consistent with the AML Rules applicable to it, to identify the source of funds and to ensure its compliance with COBS Rules 17.5(c) (Origin and destination of Virtual Asset funds) and 17.5(e) (Risk Management). These policies and procedures should cover due diligence on the deposits and withdrawals by legal persons that represent further multiple deposit-holders or withdrawal recipients of the Virtual Assets. For such deposits and withdrawals, Licensed Firms should be able to assess the ultimate beneficiaries' wallet addresses and their source or destination of funds as appropriate.

83) It is crucial that Licensed Firms perform due diligence on their Clients before opening an account so that wallet addresses can be identified as belonging to a specific user. If a transaction is detected that originates from or is sent to a "tainted" wallet address belonging to a known user, that user should be reported. Licensed Firms should maintain lists of tainted wallet addresses and, if not in possession of their own services, utilise third party services to help identify such addresses.

Planned and Unplanned system outages

84) Licensed Firms should have a programme of planned systems outages to provide for adequate opportunities to perform updates and testing. Licensed Firms should also have multiple communication channels to ensure that its Clients are informed, ahead of time, of any outages which may affect them.

85) Licensed Firms should have clear, publicly available, procedures articulating the process in the event of an unplanned outage. During an unplanned outage, Licensed Firms should be able to rapidly disseminate key information and updates on a frequent basis.

Management of personnel and decision making

86) Licensed Firms should implement processes and procedures concerning decision making and access to sensitive information and security systems.

87) A clear audit log of decision making should be kept. Staff with decision-making responsibilities should have the adequate expertise, particularly from a technological standpoint, to make such decisions.

88) Protective measures should be implemented to restrict access to critical and/or sensitive data to key personnel only. This includes both digital and physical access. Licensed Firms should have processes and procedures to track and monitor access to all network resources. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimising the impact of a data compromise. The maintenance of logs allows thorough tracking, alerting, and analysis when issues occur.

Third party outsourcing

89) Licensed Firms may use third party services for their systems. However, when doing so, an Licensed Firm (pursuant to GEN Rule 3.3.31) retains full responsibility from a regulatory perspective for any issues that may result from the outsourcing including the failure of any third party to meet its obligations. The GFSO requires that certain core systems (for example, the matching engine of an MTF using Virtual Assets) are maintained by the Licensed Firm itself and will not generally permit these to be outsourced.

90) In its assessment of a potential third party service provider, a Licensed Firm must satisfy itself that the service provider maintains robust processes and procedures regarding the relevant service (including, for example, in relation to the testing and security required in this section on Technology Governance).

91) In all circumstances, including in relation to business activities that are outsourced, a Licensed Firm is expected to maintain a strong understanding of the third-party service being provided and, for critical services, have redundancy measures in place where appropriate.

92) Public and private cloud service providers should be subject to thorough screening. A set of well-defined and documented access management procedures should be in place. All service level agreements should be reviewed annually for serviceability and security of the systems and related operations as per the IT policies of the Licensed Firm. A 'clear roles and responsibilities matrix' should be in place to delineate operations of a service provider from those of a Licensed Firm. Physical access to systems should be limited to the relevant personnel and access should be monitored by the Licensed Firm on an ongoing basis.

93) Licensed Firms are required to retain and be in the position to retrieve the data held on a cloud platform for such duration as they are required to under GFSO record keeping purposes, and submit the data held on a cloud platform to the GFSO, as and when directed to do so, with immediate effect.

94) Licensed Firms who employ cloud-based data storage services for the purpose of recording personal data must also take into consideration relevant data protection regulations. Consideration must be given to the jurisdiction within which the cloud storage service provider is located, or alternatively other arrangements which may facilitate compliance with applicable data protection requirements.

Forks

95) Licensed Firms should ensure that changes in the underlying protocol of a Virtual Asset that result in a fork are managed and tested proactively. This includes temporary forks which should be managed for reverse compatibility for as long as required.

96) Licensed Firms should ensure that their Clients are able to deposit and withdraw Accepted Virtual Assets in and out of a Licensed Firm's infrastructure as and when requested before and after a fork (except during go-live). Clients should be notified well in advance of any periods of time when deposits and withdrawals are not feasible.

97) Where the underlying protocol of a Virtual Asset (e.g., the native token of that protocol) is changed, and the new version of that Virtual Asset is backwards-compatible with the old version (soft fork), Licensed Firms should ensure that the new and old versions of the Virtual Asset continue to satisfy the relevant Accepted Virtual Asset requirements.

98) Where the underlying protocol of an Accepted Virtual Asset is changed, and the older version of the Accepted Virtual Asset is no longer compatible with the new version and/or there is an entirely new and separate version of the Virtual Asset (hard fork), Licensed Firms should ensure that client balances on the old version are reconciled with the new version of the Virtual Asset. Licensed Firms should also maintain transparent lines of communication with their Clients on how Licensed Firms are managing Clients' Virtual Asset holdings in such a scenario.

99) In the case of a hard fork, Licensed Firms should proactively manage any discrepancy between the balances recorded on the previous version versus the new version by engaging with the community which is responsible for updating and supporting the underlying protocol of the

relevant Virtual Asset. Additionally, Licensed Firms should ensure that, where they seek to offer services in relation to the Virtual Asset associated with the new version of the underlying protocol, this new Virtual Asset meets the requirements for an Accepted Virtual Asset and that they notify the GFSO well in advance of offering the Virtual Asset as part of its activities.

Virtual Asset Risk Disclosures

100) Given the significant risks to Clients transacting in Virtual Assets, Licensed Firms conducting VA Regulated Activities are required to undertake a detailed analysis of the risks and have processes in place that enable them to disclose, prior to entering into an initial transaction, all material risks to their Clients in a manner that is clear, fair and not misleading. As this disclosure obligation is ongoing, and given the rapidly developing market for Virtual Assets, Licensed Firms are required to continually update this analysis and the resultant disclosures to its Clients to reflect any updated risks relating to:

a) the Licensed Firm's products, services and activities;

b) Virtual Assets generally; and

c) the specific Accepted Virtual Asset.

101) The GFSO expects that the disclosures to be made by an Licensed Firm in order to satisfy COBS 17.6 may include:

a) Virtual Assets not being legal tender or backed by a government;

b) the values, or process for valuation of Virtual Assets, including the risk of a Virtual Asset having no value;

c) the volatility and unpredictability of the price of Virtual Assets relative to Fiat Currencies;

d) that trading in Virtual Assets may be susceptible to irrational market forces;

e) that the nature of Virtual Assets may lead to an increased risk of Financial Crime;

f) that the nature of Virtual Assets may lead to an increased risk of cyber-attack;

g) there being limited or, in some cases, no mechanism for the recovery of lost or stolen Virtual Assets;

h) the risks of Virtual Assets being transacted via new technologies, (including distributed ledger technologies ('DLT')) with regard to, among other things, anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;

i) that there is no assurance that a Person who accepts a Virtual Asset as payment today will continue to do so in the future;

j) that the nature of Virtual Assets means that technological difficulties experienced by the Licensed Firm may prevent the access or use of a Client's Virtual Assets;

k) any links to Virtual Assets related activity outside GMC, which may be unregulated or subject to limited regulation; and

l) any regulatory changes or actions by the GFSO or a Non-GFSO Regulator that may adversely affect the use, transfer, exchange, and value of a Virtual Asset.

102) For the purposes of interpreting the reference to "initial Transaction" in COBS Rule 17.6, Licensed Firms can meet the obligation in this Rule at any time prior to the 'initial Transaction'. For example, the introduction of a new Accepted Virtual Asset to trading on an MTF may require a further specific risk disclosure being made to Clients of the MTF in relation to the risks of trading in that new Accepted Virtual Asset (as assessed by the MTF).

103) The GFSO will need to understand the process by which a Licensed Firm will communicate the risks outlined in COBS Rule 17.6.2, as well as any other relevant material risks to its Clients. Where the Clients of a Licensed Firm are required to enter into a Client Agreement, the Licensed Firm may make its first such risk disclosure in that Client Agreement.

104) Considering the heightened inherent risks associated with investing in Virtual Assets and the GFSO's objective of providing a regulatory regime that offers adequate consumer protection, the GFSO is of the view that all Licensed Firms should, prior to on-boarding a Client, ensure that the services, or new services proposed to be provided to a Client are appropriate, taking into account such matters as the Client's relevant knowledge, experience and investment objectives. Where a conflict between the inherent risks and the appropriateness for a Client is identified, the Licensed Firm should take all reasonable steps to resolve such a conflict.

Market Abuse, Transaction Reporting and Misleading Impressions

105) The Market Abuse Provisions in Part 8 of the FSA specifically cover Market Abuse Behaviour in relation to Accepted Virtual Assets admitted to trading on an MTF. In this regard, the GFSO imposes the same high regulatory standards to Accepted Virtual Assets traded on MTFs as it does to Financial Instruments traded on non-Virtual Asset exchanges, MTFs or OTFs in GMC.

106) MTFs (pursuant to FSA Section 149) are required to report details of orders and transactions in Accepted Virtual Assets traded on their platforms. The GFSO may require MTFs using Virtual Assets to report to the GFSO on both a real-time and batch basis.

107) In addition, FSA provisions on Misleading Statements apply to Accepted Virtual Assets. The GFSO expects that all communications (including advertising or investment materials or other publications) made by a Licensed Firm will be made in an appropriate manner and that a Licensed Firm conducting a Regulated Activity in relation to Virtual Assets will implement suitable policies and procedures to comply with the requirements of the FSA.

108) The GFSO continues to consider developments to its regulatory perimeter in the context of its Market Abuse provisions, including for the purposes of any future determination of whether the provisions ought to be extended to further capture Virtual Asset trading activity that is not specifically linked to trading on an MTF. In this context, and particularly in the case of intermediary-type Licensed Firms, the GFSO reminds such Licensed Firms of their wider responsibilities under the Virtual Asset Framework in relation to the use of Virtual Assets, including in relation to client risk disclosures, suitability and best execution (see paragraphs 98-102, 108(a) and (b) and 114).

Application of particular Rules in the Conduct of Business Rulebook (COBS)

109) The Rules referenced in COBS Rule 17.1.4 apply to all Transactions undertaken by an Licensed Firm conducting a VA Regulated Activity. The Rules referenced in COBS Rule 17.1.4 are as follows:

a) COBS Rule 3.4 (Suitability);

b) COBS Rule 6.5 (Best Execution);

c) COBS Rule 6.7 (Aggregation and Allocation);

d) COBS Rule 6.10 (Confirmation Notes);

e) COBS Rule 6.11 (Periodic Statements); and

f) COBS Chapter 12 (Key Information and Client Agreement).

110) These requirements are relevant to the concept of 'Investment Business' within COBS and can be considered more relevant to certain Licensed Firms, particularly those that are 'dealing' in Accepted Virtual Assets. The GFSO understands that some of these obligations may not apply to all Licensed Firms (particularly MTFs using Virtual Assets).

Protection of Client Money

111) A Licensed Firm that conducts a VA Regulated Activity and which holds or controls Client Money must comply with all the relevant Client Money rules in Chapter 14 of COBS (read together with COBS Rule 17.8). Under COBS Rule 17.8.4, such Licensed Firms are required to carry out reconciliations of Client Money in Client Accounts as follows:

a) Reconciliations with respect to COBS Rule 14.11.1 shall be carried out at least every week; and

b) Reconciliations with respect to COBS Rule 14.11.4 shall be carried out within five days of the date to which the reconciliation relates.

Substance requirements of Licensed Firms

112) An Licensed Firm conducting a VA Regulated Activity must commit resources of a nature allowing it to be operating in substance within GMC. Depending on the relevant Regulated Activities being undertaken, the GFSO expects to see substantive resources committed within GMC across all lines of the Licensed Firm's activity, including, but not limited to, commercial, governance, compliance/surveillance, operations, technical, IT and HR functions. The GFSO expects the 'mind and management' of a Licensed Firm to be located within GMC. Further discussion on substance in relation to MTFs using Virtual Assets is set out in other parts of this guidance.

Virtual Asset Brokers or Dealers

113) Licensed Firms intending to operate solely as a broker or dealer for Clients (including the operation of an OTC broking or dealing desk) are not permitted to structure their broking/ dealing service or platform in a way that would have it be considered as operating a market / MTF using Virtual Assets. The GFSO would consider features such as allowing for price discovery, displaying a public trading order book (accessible to any member of the public, regardless of whether they are Clients), and allowing trades to automatically be matched using an exchange-type matching engine as characteristic of an MTF using Virtual Assets, and not activities acceptable for an intermediary-type Licensed Firm to undertake.

114) A Licensed Firm that only has an FSL to operate as a broker / dealer (in relation to Virtual Assets) and not as an MTF is required to design and structure its operations, user interface, website, marketing materials and any public or client-facing information such that it does not create the impression that it is running an MTF. In practice, this may include not displaying any publicly-accessible information that may appear like a trading order book, not providing for any price discovery, and not giving actual or potential Clients the impression that they are interacting with an MTF.

115) Virtual Asset brokers / dealers are required to comply with the best execution requirements in COBS Rule 6.5 at all times.

116) Virtual Asset brokers / dealers are required to disclose the following information to Clients:

a) How they execute and route Client's orders and source liquidity (e.g., whether they pass or route orders to other brokers, dealers or exchanges to execute). Where a broker / dealer routes Client orders to a single liquidity source such as an MTF for execution, it must also disclose this to all Clients;

b) Whether it may carry out proprietary trading on its own account, and if so, whether it may trade against Clients' positions;

c) The fees it charges Clients; and

d) How it determines the prices of the Accepted Virtual Assets it quotes to Clients

Margin trading

117) An Applicant/Licensed Firm wishing to provide margin trading to its Clients will need to submit for approval details of the terms upon which it proposes to do so (for an Applicant, in its Application – for a Licensed Firm as part of ongoing supervisory arrangements). As a general position, the GFSO would only consider allowing Applicants/Licensed Firms with a relevant proven track record to provide margin trading.

118) Particular focus will be placed on an Applicant or Licensed Firm's proposed leverage ratio.

Insurance

119) GFSO recommends that Virtual Asset brokers/dealers and Virtual Asset Custodians take out insurance policies with respect to the Virtual Assets they hold on behalf of clients. As a first line of defence, the GFSO expects all Licensed Firms to ensure the proper structuring of their business operations and to implement robust mechanisms for the mitigation of actual and potential areas of risk.

SPECIFIC REQUIREMENTS FOR MULTILATERAL TRADING FACILITIES

Background

120) The GFSO considers Operating a Multilateral Trading Facility with respect to Virtual Assets to be a key VA Regulated Activity in GMC.

Substance requirements for MTFs

121) Consistent with the treatment of all Licensed Firms, the GFSO requires MTFs to be based in substance within GMC. In addition to the substantial commitment of resources required of an MTF Operator, this also means that the GFSO's regulatory oversight of an MTF extends to its order book, matching engine, rulebook(s), ensuring fair and orderly markets, settlement, and for the purposes of preventing/monitoring for Market Abuse, amongst the relevant requirements set out in the Market Infrastructure Rulebook ("MIR") and COBS Chapter 8.

122) In practical terms, this means that for a start-up MTF, its entire order book and the functionality of its matching engine will be subject to GFSO oversight. For existing operational virtual asset exchanges that already have their order book / matching engine outside GMC prior to making an application, a determination of which parts (if not all) of its order book (and how its matching engine) will come under GFSO regulatory oversight needs to be made by the Applicant, to allow it to apply to become licensed as an MTF.

123) In situations where an entity establishes an Licensed Firm that routes orders to a virtual asset exchange outside GMC (even as part of a Group that may be operating globally) instead of having orders matched within an MTF's order book within GMC, that entity cannot obtain an MTF Exchange license within GMC and can only be licensed as an intermediary-type Licensed Firm within GMC.

124) Chapter 8 of COBS also contains the requirements for the operation of an Organised Trading Facility (OTFs). The application of OTF Rules, however, are not relevant to the operation of Virtual Assets.

Guidance in relation to Applicable Rules for MTFs

125) In addition to the MTF Rules set out in COBS Chapter 8, MTFs are also required to meet the requirements set out in COBS Rules 17.1 to 17.6, and the additional Rules set out in COBS 17.7.

126) Chapter 8 of COBS incorporates Rules from various other GFSO Rulebooks that must be complied with, including certain sections of MIR. COBS Rule 8.2.1 sets out various Rules in MIR that MTFs (using Virtual Assets) are required to comply with to the satisfaction of the GFSO, with the applicable Rules set out as follows:

a) MIR Rule 2.6 (Operational systems and controls): MIR Rule 2.6.1 requires an MTF to 'establish a robust operational risk management framework with appropriate systems and controls to identify, monitor and manage operational risks that key participants, other [MTFs], service providers (including outsourced) and utility providers might pose to itself.'

b) In relation to systems and controls, the GFSO has provided guidance on what it expects in relation to technology governance controls in this Guidance. The GFSO therefore requires an MTF to undertake its 'MTF' activities in compliance with these operational system and control requirements, in combination with the technology governance controls outlined earlier in this Guidance.

c) The GFSO expects an MTF to undertake extensive due diligence and testing of its operational systems and controls, with the relevant reports of such testing capable of being provided to the GFSO for review. Such testing should be undertaken by an officer of the MTF possessing appropriate skills and experience. The testing reports need to confirm the robustness of the MTF's systems and address any potential areas of failure. Testing should include the settlement processes for the movement of Virtual Assets between wallets, and the general connectivity of the MTF's systems with other parties. Testing should be ongoing, building in processes for the introduction of new Accepted Virtual Assets.

d) An MTF will need to provide policies and procedures that clearly evidence how it will effectively address a failure of its systems. Failures must be rectified as soon as practicable, with an MTF's business continuity plan including detailed and realistic response timeframes for failures or disruptions.

e) MIR Rules 2.7.1 and 2.7.2 (Transaction recording): GFSO expects that the primary ledger technology systems and controls of an MTF (whether they be DLT or multiple-ledger technologies) will be such that transaction recording and reporting is easily facilitated, and that all GFSO requirements can be effectively complied with. Where reconciliations are required to be undertaken, for example, between a DLT based ledger and an internal ledger maintained by an MTF for the purposes of transactions and/or settlement, the GFSO will need to be satisfied that the reconciliation process is robust, timely and efficient.

f) MIR Rule 2.8 (Membership criteria and access): MIR Rule 2.8.1 requires that an MTF 'must ensure that access to its facilities is subject to criteria designed to protect the orderly functioning of the market and the interests of investors'.

Market Access and Surveillance for MTFs

127) MIR Rules 2.8.2, 2.8.3, 2.8.5 and 2.8.6 support the operation of MIR Rule 2.8.1, and the GFSO expects that MTFs consider the application of the requirements across these Rules - for example, MIR Rule 2.8.5 contains substantive provisions that should apply, regardless of what model of 'access' an MTF (using Virtual Assets) utilises.

128) The GFSO recognises, however, that MTFs (using Virtual Assets) generally operate a 'direct access' model that does not involve Members (e.g. access to the exchange is not intermediated by broker-dealers in the traditional securities exchange model). Instead, clients of an MTF trade directly on the platform. An MTF operating in this manner will, therefore, need to ensure that it has appropriate processes, controls and rules to 'protect the orderly functioning' of its market, its facilities and the interests of its investors.

129) By not adopting a 'Member-access' model and allowing 'direct access', MTFs lose one layer of regulatory/supervisory defense that traditional securities exchanges and Member-access MTFs have, in that they do not have Members assisting them in the undertaking of the necessary due diligence and compliance reviews of investors being on-boarded into their market. The GFSO, in these circumstances, requires MTFs to undertake their own CDD reviews for every client accessing (trading on) their market. Resultant AML/CFT obligations therefore fall on the MTF itself.

130) MIR Rule 2.9 (Financial crime and market abuse): MTFs are required to operate an effective market surveillance program to identify, monitor, detect and prevent conduct amounting to market misconduct and/or Financial Crime. Given the significant risks, and the nascent nature and constant pace of development of the Virtual Asset industry, an MTF's surveillance system will need to be robust, and regularly reviewed and enhanced.

131) The GFSO further reminds MTFs, and investors trading on an MTF, of the Market Abuse provisions applicable to the trading of Accepted Virtual Assets on an MTF.

132) MIR Rule 3.3 (Fair and orderly trading): MIR Rules 3.3.1 to 3.3.4 establish the requirements an MTF must meet for providing fair and orderly trading across its market, and for having

objective criteria for the efficient execution of orders. The GFSO considers these requirements to be fundamental to the operation of an MTF.

133) MIR Rule 3.8 (Settlement and Clearing Services): An MTF will need to have clear processes in place for the settlement (and if applicable, the clearing) of all Accepted Virtual Asset transactions. As noted in the AML and Technology Governance sections of this Guidance, extensive stress testing on capabilities to connect successfully with third parties, and in relation to the movement of Accepted Virtual Assets between wallets, will be required to be undertaken to the GFSO's satisfaction. The GFSO will not necessarily require a connection to a separate Recognised (or Remote) Clearing House where the MTF can demonstrate that it has in place 'satisfactory arrangements for the timely discharge, Clearing and settlement of the rights and liabilities of the parties to transactions effected' on the MTF, including where it is utilising the services of a Virtual Asset Custodian.

134) MIR Rule 3.10 (Default Rules): Depending on whether an MTF operates a 'Member-access' model or it allows direct 'Client-access' will determine the full, or partial, application of MIR Rules 3.10.1 to 3.10.3. The GFSO, at a minimum, expects MTFs to have in place both rules and a process to suspend or terminate access to its markets in circumstances where a Client/Member is unable to meet its obligations in respect of transactions relating to Accepted Virtual Assets.

135) The GFSO suggests that an Applicant/Licensed Firm consider different scenarios/circumstances where it may need to utilise the powers provided to it under its Default Rules, and take appropriate action as required. Scenario testing of this kind could relate to when there is a financial and/or technical 'default' in relation to, for example, its custody, fiat token or wider banking arrangements. Due to a prevalence of pre-funding of (client) positions within Virtual Asset markets, the impact of a 'default' in such a scenario may not necessarily be on a per-transaction basis, but could be structural in nature, in limiting the ability of Clients to fund their positions (and therefore the ability of the MTF to operate on a fair and orderly basis).

136) To prepare for the event of a loss/default, the GFSO expects an MTF to have, within its policies, a clear process for the management of such loss (e.g., what is the exposure of individual Clients, counterparties, its Custodian and itself, as applicable).

137) COBS Rule 17.7.4 specifies that certain notification requirements applicable to Recognised Investment Exchanges under MIR Rules 5.1, 5.3 and certain information requirements under MIR Rule 5.4.1 apply to MTFs (using Virtual Assets). These are additional requirements applicable to MTFs using Virtual Assets. MTFs using Virtual Assets will also need to comply with any other applicable notification requirements, including those set out in the Accepted Virtual Assets section of this Guidance in relation to the use of additional Accepted Virtual Assets.

Custody Arrangements Used by MTFs

138) It is recognised that MTFs may take varying approaches in relation to the custody of Virtual Assets. An MTF may use third party custodians but still be holding itself out to its Clients as

being responsible for custody of their Accepted Virtual Assets. Alternatively, an MTF may provide custody of Clients' Accepted Virtual Assets wholly itself, done "in-house" without the use of any third-party custodians. An MTF whose custody arrangements fall into either of these two scenarios will also be considered to be Providing Custody of Virtual Assets for the purposes of the Virtual Asset Framework and will be required to comply with COBS Chapters 15 and 16, and take guidance from the section below on "Licensed Firms Providing Custody of Virtual Assets".

139) As further set out in paragraphs 153 and 154, in circumstances where an MTF is also Providing Custody, the GFSO expects appropriate segregation of responsibilities, staff, technology and, as appropriate, financial resources, between the operations of the MTF and the Virtual Asset Custodian.

Traditional Securities Exchanges Operating an MTF using Virtual Assets

140) Pursuant to MIR Rule 3.4.1, a traditional securities exchange may operate an MTF, provided that the GFSO permits it to do so. MIR Rule 3.4.2 requires that where such a stipulation is granted, the traditional securities exchange must meet the requirements of the Virtual Asset Framework in relation to operation of an MTF (using Virtual Assets) while the remainder of its operations must be operated in compliance with the MIR Rules.

141) This means that a traditional securities exchange (in addition to operating markets relating to the trading of Financial Instruments (including Digital Securities) can, where permitted by the GFSO and subject to MIR Rule 3.4.2, operate a separate MTF, OTF and/or MTF using Virtual Assets under its Recognition Order.

SPECIFIC REQUIREMENTS FOR LICENSED FIRMS PROVIDING CUSTODY OF VIRTUAL ASSETS

142) Licensed Firms (including MTFs) Providing Custody in relation to Virtual Assets ("Virtual Asset Custodians") provide the service of helping Clients safeguard their Accepted Virtual Assets. Virtual Asset Custodians include firms that solely offer the custody of Virtual Assets for Clients, as well as MTFs and other intermediaries who additionally provide the service of custodizing Accepted Virtual Assets on behalf of Clients.

143) Similar to the approach taken in relation to activities undertaken by MTFs in relation to Virtual Assets, the GFSO considers the activities undertaken by Virtual Asset Custodians to be a key VA Regulated Activity within GMC. Accordingly, the Virtual Asset Framework contains specific additional requirements applicable to Virtual Asset Custodians.

144) Virtual Asset Custodians are required to comply with Chapter 15 (read together with COBS Rule 17.8) and Chapter 16 of COBS at all times. Virtual Asset Custodians are also required to comply with COBS Rules 17.1 to 17.6. Licensed Firms should also note that COBS 17.8.2 requires that "Investment" or "Investments", (and, as a result, the corresponding references to

"Client Investments") be read as encompassing "Virtual Asset" or "Virtual Assets", as applicable. This means that a Licensed Firm that holds, controls, or Provides Custody for, Accepted Virtual Assets, on behalf of their Clients must comply with all relevant Safe Custody rules in Chapter 15 of COBS (read together with Chapter 17 of COBS) at all times. This approach has been taken by the GFSO to ensure that Accepted Virtual Assets are afforded the same protections as other similar products and activities under FSA and the GFSO Rulebooks.

145) Under COBS 17.8.3, Virtual Asset Custodians are required to carry out all reconciliations of a Client's Virtual Asset holdings at least every week (as required under COBS Rule 15.9.1).

Custodial Arrangements for Clients' Virtual Assets

146) The GFSO notes that there are various custody arrangements that firms may use to hold virtual assets for their Clients:

a) One common arrangement is where a firm custodizes virtual assets for their Clients using either the firm's own proprietary wallets, or uses wallet technology purchased from third party wallet providers. In such an arrangement, as the wallets holding Clients' virtual assets are wholly under the control of the firm, the firm would be deemed as carrying out the regulated activity of Providing Custody and would require an FSL from the GFSO.

b) Another arrangement is an outsourcing-type one where a firm ("Firm A") custodizes virtual assets for their Clients by using third party virtual asset custodians. Such third party virtual asset custodians will hold on the virtual assets of Firm A's Clients on trust. Notwithstanding that the wallets holding the virtual assets are under control of the third party virtual asset custodian, Firm A would still be deemed as carrying out the regulated activity of Providing Custody and would require an FSL from the GFSO. The GFSO would generally expect Licensed Firms adopting this model to use third party virtual asset custodians which have strong internal controls and are suitably licensed for their custody activities.

. Where a Licensed Firm outsources part or all of the custody function to a third party, the Licensed Firm is required to perform its due diligence and background checks on the third party, and ensure that the third party meets all the GFSO's requirements applicable to Virtual Asset Custodians. Such Licensed Firms are required to make full disclosures to their Clients and to the GFSO regarding such outsourced custody arrangements. The Licensed Firm retains full responsibility from a regulatory perspective for any issues that may result from such outsourcing, including the failure of any third party to meet its Virtual Asset Custody obligations.

c) Wallet providers which merely sell virtual asset wallets and do not have unilateral control over the virtual assets held in such wallets would not be deemed as providing custody and hence not require an FSL from the GFSO.

Governance Arrangements for Virtual Asset Custodians

147) From a governance perspective, a Virtual Asset Custodian should have proper governance structures in place to avoid or mitigate actual or potential conflicts of interest between its custody functions and any other activities or functions within itself or with other Group entities. Such governance arrangements may include having a separate team, which does not have other conflicting responsibilities within the firm, handling custody.

148) Licensed Firms operating as Virtual Asset Custodians must not, at any time, permit arrangements whereby just a sole party or signatory is able to completely authorise the movement, transfer or withdrawal of Accepted Virtual Assets held under custody on behalf of Clients. In particular, Licensed Firms must not have custody arrangements whereby only a sole person can fully access the private key or keys for the Accepted Virtual Assets held under custody by the Licensed Firm. Preventing such arrangements can help reduce potential key person risk such as theft, fraud, unwillingness or inability of the sole party to grant access to private keys.

149) Licensed Firms are also required to mitigate the risk of collusion between all authorised parties or signatories who are able to authorise the movement, transfer or withdrawal of Accepted Virtual Assets held under custody. Licensed Firms are required to provide information on these mitigating controls to the GFSO.

150) Licensed Firms are required to have policies and procedures in place that clearly describe the process that will be adopted in the event that it knows or suspects that the Accepted Virtual Assets it is holding under custody on behalf for Clients has been compromised, such as in the event of a hacking attack, theft or fraud. Such policies and procedures should detail the specific steps the firm will take to protect Clients' Accepted Virtual Assets in the event of such incidents. Licensed Firms should also have the ability to immediately halt all further transactions with regard to the Accepted Virtual Assets.

STABLECOINS

151) The GFSO has implemented a dedicated framework for the issuance of Fiat-Referenced Tokens ("FRTs"). A FRT is a digital asset, the transfer and storage of which is achieved through the use of distributed ledger or similar technology, the purpose of which is to be used as a medium of exchange with a stable store of value, by:

a) referencing a fixed amount of a single fiat currency; and

b) enabling the holder to redeem the token in exchange for the amount of the fiat currency referred to in a) from its issuer upon demand.

152) COBS 17.2.1 also requires that a Licensed Firm carrying on a Regulated Activity involving an FRT must only use Accepted FRTs (i.e., those which have been approved by the GFSO). Persons seeking to carry on a Regulated Activity involving FRTs, including those seeking to

issue FRTs in GMC, should consult relevant Rules and Guidance relating to FRTs, including Chapters 17 and 19A of COBS.

153) The GFSO recognises that not all assets described as 'stablecoins' will satisfy the definition of an FRT. For example, a 'stablecoin' may aim to maintain a stable value relative to an asset(s) other than a single fiat currency and so will not satisfy the definition of FRT. Persons seeking to carry on a Regulated Activity involving an asset described as a 'stablecoin' but which does not satisfy the definition of an FRT should contact the GFSO to discuss the regulatory treatment of the specific asset in question.

APPLICATION PROCESS FOR FIRMS SEEKING A FINANCIAL SERVICES LICENCE IN GMC WITH RESPECT TO VIRTUAL ASSETS

154) Applicants seeking to become a Licensed Firm conducting a VA Regulated Activity must be prepared to engage heavily with the GFSO throughout the application process. The application process is broadly broken down into five stages, as follows:

a) First contact the GFSO at gfso@gmc.bt to arrange an initial meeting.

b) At the initial meetings, you will need to present your proposed business model and its risks, and explain why you wish to set up in GMC. Subject to the outcome of these initial meetings, the GFSO may invite you to submit an application for a Financial Services Licence and send you the application form(s).

c) When you submit your application form(s), the GFSO will issue the invoice for the non-refundable application fee you are required to pay. Refer to the following section in this Guidance on fees.

d) The GFSO will review your application and request meetings with you where required. This may include interviewing key personnel from your business.

e) If your application is successful, you will receive an In-Principle Approval ("IPA") containing a number of pre-conditions you must satisfy before you are issued the actual Financial Services Licence. Note that the IPA does not permit you to conduct your business in GMC yet.

f) You must fulfill the IPA conditions, which will include incorporating a company in GMC via the Gelephu Corporate Registration Office ("GCRO") department within the GMCA, opening a bank account in GMC, injecting the required regulatory capital, obtaining office space in GMC, hiring key personnel, etc.

g) Once you have fulfilled all IPA conditions, the GFSO will issue the Financial Services Licence to you, which allows you to commence your business in GMC.

FEES

155) The table below shows the application and annual supervision fees payable by firms carrying out regulated activities with respect to virtual assets.

Regulated Activity	**Application Fee Per Regulated Activity**	**Annual Supervision Fee Per Regulated Activity**
Carrying out regulated activities[1] with respect to Virtual Assets *(other than Operating a Multilateral Trading Facility - see below)*	US$5,000	US$5,000
Operating Multilateral and Organised Trading Facilities (i.e. a stock exchange or crypto exchange)	US$50,000	US$50,000

156) Note that fees are cumulative. For example, a firm that seeks to provide virtual asset brokerage and custody services in GMC would likely need to apply for an FSL with respect to the following two regulated activities:

a) Dealing in Investments

b) Providing Custody

The one-time application fee for these two regulated activities would be US$10,000, and the ongoing annual supervision fee would then be US$10,000 paid annually. The annual supervision fee will be prorated based on the number of months left in the year.

[1] See the GMC Financial Services Act's Schedule 1 (Regulated Activities: Part 1) from page 252 onwards for the list of regulated activities.