.

VANUATU FINANCIAL SERVICES COMMISSION

GUIDANCE NOTES

ON

RISK MANAGEMENT

SUPERVISION DEPARTMENT

GUIDE ON RISK MANAGEMENT

PART 1

1. INTRODUCTION

These Guidelines are issued under Section 19A of the Financial Dealers Licensing Act as amended (the Act).

The purpose of this guideline is to set out the high level principles for Financial Dealers to identify and manage their inherent risks. Each licensee is required to submit a written Risk Management policy and procedure to VFSC covering all identified inherent risk and the mitigating factors put in place to manage those risks. The high level principles for risk management would be subject to regular update and amendment, as required. Amendments to risk management document are to be approved by the Board of Directors. The risk management document must be reviewed at least annually in connection with changes in the technology, market environment and when maximum limits for risk exposure are reviewed and amended.

2. DEFINITION OF RISK MANAGEMENT

Risk Management is the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk. It is important that employees and directors of the Company manage risk for the benefits of its stakeholders.

3. STRATEGY TO MANAGE RISK

A holder of Class A, B, C and D license must have a sound strategy to manage risks arising from its core business activities. The licensee should first determine its risk tolerance, i.e. the level of risk that it is able and prepared to bear, taking into account its business objectives and available resources. In formulating its risk management strategy, the licensee should consider the following:

a). the prevailing and projected technology, economic and market conditions and their impact on the risks inherent in its core activities;

b). the available expertise to achieve its business targets in specific market segments and its ability to identify, monitor and control the risks in those market segments; and

c). its mix of business/type of risks undertaken and the resulting concentration risks which may lead to volatility in business income and profitability.

A licensee should periodically review its risk management strategy taking into account its own financial performance and market developments. When there

are material changes to its operations or its business strategy, the Licensee should review its risk management strategy appropriately to take account of the changes. The strategy should be properly documented and effectively communicated to all relevant staff. There should be a process to approve proposed deviations from the approved strategy, and systems and controls to detect unauthorised deviations.

4. STRUCTURE

A Licensee should adopt a risk management structure that is commensurate with its size and nature of its activities. The organisational structure should facilitate effective management oversight and execution of risk management and control processes.

The Board of Directors is ultimately responsible for the sound and prudent management of a licensee. The Board should approve the risk management strategy and risk policies pertaining to core business activities. It should ensure that adequate resources, expertise and support are provided for the effective implementation of the licensee's risk management strategy, policies and procedures. It should also be the approving authority for changes to such policies, and ensure that any exceptions, which can include circumstances where delegation may be proposed, should be escalated and approved by it, where necessary. The reasons for these changes and exceptions should be documented. Such documentation should also be available upon request to the external auditor and the regulator.

The senior management, or a committee comprising members of senior management from both the business operations and control functions, should establish the risk management framework. The framework should cover areas such as approval of business and risk strategy, review of the risk profile, implementation of risk policies approved by the Board, delegation of authority and evaluation of the business processes. There should be adequate measures to address potential conflicts of interest. For example, the member of senior management approving the base rate of investment in securities product should not have marketing responsibilities and there should be proper segregation of responsibilities from client investment handling and settlement responsibilities.

A licensee should establish a risk management function, preferably independent from the operational processes, if warranted by the size and complexity of its operations. This function would be primarily responsible for the development of and ensuring compliance with the licensee's risk management policies and procedures.

5. POLICIES AND PROCEDURES

Risk policies should set out the conditions and guidelines for the identification, acceptance, monitoring and management of risks. These policies should be well-defined and consistent with the licensee's risk strategy, as well as adequate for

the nature and complexity of its activities. They should also help explain the relationship of the risk management system to the company's overall governance framework and to its corporate culture. The policies should, at a minimum, cover the following:

a.) the identification, measurement and communication of key risks to the Board;

b). the process by which the Board decides on the maximum amount of risk the company is able to take, as well as the frequency of review of risk limits;

c) the roles and responsibilities of the respective units and staff involved in acceptance, monitoring and management of risks;

d). the approval structure for product development, pricing, investment underwriting, and handling of payment settlements, including authority to approve deviations and exceptions;

e). the management of concentration risk and exposures to catastrophic events, portfolio monitoring and stress testing.

In order to be effective, policies should be communicated regularly throughout the organisation and should be revised periodically to take into account changing internal and external circumstances. There should also be regular training on risk policies.

The licensee should establish appropriate procedures and processes to implement its risk policies in the form of controls, checks and monitoring mechanisms. These should be documented and set out in sufficient detail to provide operational guidance to staff.

The licensee should have in place proper and effective reporting systems to satisfy the requirements of the Board with respect to reporting frequency, level of detail, usefulness of information and recommendations to address issues of concern. There should be clear guidelines on the type of information to be reported to the Board on a regular basis as well as when certain information or development ought to be communicated immediately to the Board. The head of risk management function should have the authority and obligation to inform the Board promptly of any circumstance that may have a material effect on the risk management system of the licensee.

6. RISK IDENTIFICATION, CONTROL AND MONITORING

Types of Risk and Risk Mitigation Techniques

The following are some of the main risks associated with securities transactions. Best practices for mitigating each of these risks are also described. Best practices for mitigating risk apply where a licensee through its manager or representative is entering into a securities transaction or where external investment managers have been delegated authority to enter into securities transactions on behalf of the licensee. Before delegating authority to an external investment manager to enter into a derivative transaction, the licensee should exercise appropriate due diligence to ensure that the external investment manager has established best practices for risk mitigation.

The sophistication of the approach to mitigating risk should match the investment types, use of securities and the complexity of the transactions entered into. The best practices for risk mitigation described below under the various risk categories should be considered by the licensee and documented in the licensee's risk management framework, as appropriate.

7. Market Risk

Market risk is the risk of financial loss arising from adverse changes in the market value (price) of the reference asset or instrument that underlies the securities transaction. Market risk can be influenced by many factors, including movements in interest rates, credit spreads, equity prices, exchange rates or commodity prices. Licensee should pay particular attention to derivative transactions that involve the use of leverage, as these transactions can increase market risk by magnifying losses.

Mitigating Market Risk

To manage market risk, Licensees should consider the following:

Monitoring Market Risk and Leverage

Securities transactions can expose investment plans to market risk from a range of sources, and the amount of exposure can greatly exceed the plan's initial investment. Market risk can be increased due to the significant leverage effect of certain securities. For example, a minor fluctuation in the value of the underlying interest can potentially cause large fluctuations in the value of a derivative. The value of a derivative that has a leverage effect can, therefore, be highly volatile.

Licensees should ensure that any securities transactions that involve the use of leverage are understood and closely monitored and managed in order to avoid undue risk. Limits should be established for the amount of leverage that the licensee may obtain through securities transactions that are consistent with maximum exposures authorized by the Licensee's risk management framework. When establishing limits on the use of leverage, licensee should take into account the company's overall exposure from all of the leveraged investment strategies that the licensee has entered into. Setting limits would allow the licensee to assess the maximum financial loss in the most extreme market conditions. These limits should be clearly understood by all parties who are authorized to enter into derivative transactions on behalf of the plan. Plan

administrators should carefully consider the use of leverage when using derivatives since losses can be greater than the money put into these instruments.

8. Counterparty Credit Risk

Counterparty credit risk is the risk of loss due to a counterparty's unwillingness or inability to pay its contractual obligations under a contract. When a licensee enters into a non-centrally cleared OTC transaction, the licensee takes on the risk that their counterparty will default, causing the loss of market exposure or hedge provided by the investment transaction and potentially the loss of any unrealized gain from open financial investment contracts. Prudent management of counterparty credit risk can help minimize the risk of loss in the event of a counterparty default.

Mitigating Counterparty Credit Risk

To manage counterparty credit risk, the licensee should consider the following:

Credit Assessments

Counterparty credit risk can be managed through appropriate measurement of exposures, ongoing monitoring, timely evaluations of counterparties, and sound operating procedures. Before entering into a non-centrally cleared OTC securities contract, the licensee should conduct a comprehensive credit assessment of each of its proposed counterparties. Credit limits should be established for each counterparty, taking into account factors such as the creditworthiness of the proposed counterparty and whether collateral arrangements will be in place.

9. Liquidity Risk

Licensees who use derivatives are faced with two types of liquidity risk:

- **Market liquidity risk**: the risk that the licensee may not be able to exit or offset a derivatives position quickly or at a reasonable price. This inability may be due to inadequate market depth or stressed market conditions.

- **Funding liquidity risk**: the risk that the licensee may not be able to meet the future cash flow obligations from its derivative transactions such as meeting margin calls. Whether the derivatives are exchange traded or OTC derivatives, changes in the mark-to-market value of the derivative may result in the receipt of collateral or the need to post collateral on a daily basis. Licensee will therefore need to ensure that a sufficient supply of liquid, eligible collateral instruments is on hand to satisfy potential margin or collateral calls and that the licensee has the required operational and management capabilities to manage these transactions.

Mitigating Liquidity Risk

The licensee's risk management framework should address the processes and procedures by which liquidity risk is managed. These processes and procedures should include the following:

a). Prior to entering into a securities transaction, considering the market depth of the security transaction

b). Monitoring market depth for securities transactions on an ongoing basis

c). Ensuring that when collateral is pledged, the Licensees liquidity is not compromised and the pension fund's overall risk profile is not adversely affected

d). Ensuring that sufficient cash reserves and cash equivalent instruments are maintained by the licensee to meet potential collateral demands.

10. Operational Risk

Operational risk is the risk of loss resulting from the actions of people, inadequate or failed internal processes and systems, or from external events. This is a particular risk in securities activities because of the complex and rapidly evolving nature of some financial or securities strategies. Operational risk also includes legal risk. Legal risk is the risk that a security or financial contract will not be legally enforceable. A number of factors contribute to legal risk, including the following:

a). The legal capacity and authority of a counterparty to enter into a securities or financial contract

b). The securities or financial contract documentation being deficient or unenforceable

c). The securities or financial transaction not being in compliance with regulatory requirements.

Mitigating Operational Risk

The controls in place to manage operational risk must be commensurate with the scale and complexity of the financial activity being undertaken. Before entering into a securities transaction, a licensee should ensure that there are processes and procedures in place that demonstrate the following:

a). That systems can support, and operational capacity can accommodate, the types of financial or securities transactions that the plan administrator is authorized to engage in;

b). That all relevant details of securities or financial transactions are documented;

c). That there is sufficient staff with the expertise to support the volume and types of complex securities transactions that the licensee may enter into;

d). That staff who are involved with making decisions regarding the use of securities products such as derivatives will be provided with on-going education;

e). That the methods for valuing positions are appropriate and the assumptions underlying valuation methods are reasonable.

11. Legal Due Diligence

Prior to entering into a financial transaction, a Licensee should satisfy itself that the counterparty to the transaction has the regulatory and legal authority to enter into the transaction. A Licensee should also be satisfied that the terms of the transaction are adequately documented and legally enforceable. This is especially important with respect to provisions concerning the timing of the termination of outstanding transactions and the calculation of settlement amounts payable to or between parties upon the termination of the transaction. In order to promote legal certainty, a licensee should agree in writing to all material terms governing their trading relationship with their counterparty prior to or at the time of execution of a transaction.

12. Regulatory Compliance

A licensee should be aware that they and/or their counterparties may be subject to specific regulatory requirements for registering, central clearing, risk mitigation and trade reporting if they transact in securities;

Given the global nature of securities markets, Licensees should have procedures for identifying, communicating, managing and mitigating regulatory compliance risk. Licensees should also maintain knowledge of the regulatory requirements that apply to their securities activities, for all relevant jurisdictions.

13. Conducting Stress Testing

Licensees should, as appropriate, conduct stress testing of the securities or financial investments transactions under various market conditions and scenarios. Licensees should incorporate within the stress testing procedures the likelihood of adverse events affecting investment exposures (including adverse market movements, heightened counterparty credit or liquidity risks, or other possible events) to ensure that the licensee is aware of potential losses that the entity is exposed to from its financial transactions.

Stress testing helps to identify how the investment portfolio and liabilities respond to shifts in relevant economic variables or risk parameters. The sophistication of Licensee's stress testing should be proportionate with the size and complexity of the investment activities.

14. Best Practices

The prudent use of securities and financial instruments has the potential to enhance investment returns and reduce risks. If not used properly, however, securities can lead to substantial losses. In order to use these instruments effectively, Licensees must understand how securities or financial instruments can alter the risk and return profile of the investment plan and investment fund, and have a sound risk management framework to prevent unintended consequences.

Each entity has considerable choice regarding how they monitor and manage risk. At the same time, derivative strategies and investment portfolio compositions

have become increasingly complex – which in turn requires more sophisticated risk management policies and procedures. This makes it even more important for Licensees to understand, monitor and manage their risk exposures. As risk management practices for securities or financial instruments are constantly evolving, VFSC expects each Licensee to remain current with best practices and to adopt such practices as applicable.

PART 2

Risks involved in trading and custody of digital assets

1 Introduction

This Digital Asset Risk Document is separate from and in addition to the disclosure of risk factors by issuers, distributors, counterparties or other persons and financial services providers involved in the issuance, distribution, trading and other transactions relating to Digital Assets, as may in particular be contained in prospectuses, key information documents, white papers, fact sheets and other information sheets and which describe in more detail the risks associated with a particular Digital Asset or category of Digital Asset.

This document does not constitute nor purport to constitute exhaustive disclosure of all relevant risks or other relevant aspects in connection with Digital Assets or transactions in such assets. It is a guide only for the regulatory framework to be put in place and ascertain risk factors of the products and services in the financial services sector and non-bank related activities.

2. **Reasons for investments in Digital Assets**

The reasons for investing in Digital Assets are unique to each client. However, the following reasons can be cited among others:

a). Diversification: some Digital Assets, such as payment tokens, can show low correlation with traditional asset classes, and, as such, can bring diversification benefits in an overall portfolio context.

b). High risk / high return profile.

c). Belief in distributed ledger technologies: there is a consensus that distributed ledger technologies have a similar potential to that of the Internet 20 years ago.

d). Loss of confidence in the traditional monetary system.

e). Betting on the future: the future of Digital Assets is still largely unknown.

3. **Key characteristics**

Before investing, the Client should know some key elements related to Digital Assets. The elements presented below are only a part of them.

a. Distributed Ledger Technology

Distributed Ledger Technologies (″DLT″) refers to technologies that allow individual participants (nodes) within a system to propose, validate, and store operations in a synchronised dataset (″Ledger″) that is distributed across all nodes in the system securely. It typically exhibits the following characteristics:

- ***Embedded consensus algorithm***

  A distributed ledger includes a ″consensus algorithm″ that allows to add and replicate new entries in the database without any trusted third-party validation. In other words, none of the computers making the network needs to be trusted and the consensus algorithm makes sure that all the data entered is accurate.

- ***Decentralised infrastructure***

  A distributed ledger has no single point of failure, which means that if multiple computers participating in the network disappear, the network will continue to function if there is one computer.

- ***Decentralised governance***

  A distributed ledger has no single entity controlling the network or making the rules for the network. The rules are defined in the ″code″ running the distributed ledger.

- ***Logically centralised***

  A distributed ledger is logically centralised which means that every node sees the same state. It can be seen as a one global computer or thousands of dispersed computers that all see the same state.

Blockchain is a possible form of how data can be stored in such a system: operations (e.g., transactions) are organised in blocks, and a block is attached to the last previously created block. This allows operations and data to be stored without allowing them to be subsequently modified.

There are two main types of distributed ledgers:

- *Permissionless or public distributed ledgers*

  Anybody, incl. private individuals, can participate in the network by installing the relevant version of the software. Examples are Bitcoin, Ethereum, Ripple etc.

- *Permissioned or private distributed ledgers*

  Only people invited or accepted to join the network can do so – they need the permission of a trusted authority. Examples are hyperledger, R3 corda or other enterprise blockchain services.

b. Digital Assets

Digital Assets are digital representations of any types of assets, securities, rights, currencies or units of accounts registered on a distributed ledger such as a blockchain. They include but are not limited to cryptocurrencies such as Bitcoin, Ethereum or Litecoin. They can also include securities such as classical shares or bonds registered on a distributed ledger (i.e. “tokenised securities” registered on a “securities ledger”).

From a regulatory perspective, regarding the regulatory framework for initial coin offerings (“ICOs”) Digital Assets can be classified in four categories: payment tokens, utility tokens, asset/security tokens and hybrid tokens.

For the purposes of this paper, they will not be discussed at length as at present regulation is not allowing. In that been said,the individual token classifications are not mutually exclusive. Asset/security and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). In these cases, the requirements are cumulative; in other words, the tokens are deemed to be both securities and means of payment.

4. How to invest in Digital Assets?

Investors can buy themselves digital assets (for example through websites, crypto-currency exchanges, trading applications) or through selected banks and/or brokers.

5. Main risks

The following list highlights some of the main risks linked to digital assets, without being exhaustive:

Volatility risk

- The value of Digital Assets is subject to high volatility, i.e., the price of Digital Assets may rapidly go down as well as up, on any given day, including on an intraday basis. Investments in Digital Assets are deemed highly speculative investments. The risk of substantial or total loss in purchasing or selling Digital Assets exists.
- Market prices may be very volatile and sometimes differ materially from the fair value of a Company or an investment opportunity in the case of illiquid/low liquidity assets.
- While the volatility of Digital Assets is high and varies significantly, changes and advances in technology, fraud, theft and cyber-attacks and regulatory changes, among others, may increase volatility further – elevating the potential of investment gains and losses. In addition, Digital Assets lack the historical track record of other currencies or commodities such as gold that could guide if current levels of volatility are typical or atypical.

Valuation risk Setting a value to Digital Assets can be difficult depending on which category is chosen and, in some cases, there may not be any proven valuation methods:

a). Payment tokens: the price of payment tokens depends on the supply and demand dynamics on a global level and does not rely on traditional valuation techniques used for securities (e.g., discounted cash flows), which can make it hard to provide an objective value to payment tokens.

b). Utility tokens: utility tokens represent a right to consume a service or a product in the future. There are no proven valuation methods. Some of the utility tokens that are being issued have no intrinsic value other than the possibility to use them to access or use a service/product that is to be developed by the issuer. There is no guarantee that the services/products will be successfully developed. At the time of writing, the Company is not planning to provide access to utility tokens.

c). Asset/security tokens: discounted cash-flow analysis + liquidity or illiquidity premium depending on i) maturity of company ii) trading venues. Asset tokens bear risks related to the underlying Company or asset in particular liquidity as many of the Companies raising funds are private Companies not listed in a stock market. See the Swiss Bankers Association standardized information booklet for further details on liquidity risks. Digital Assets only exist virtually on a computer network and have no physical equivalent. Establishing a value for Digital Assets is difficult as the value depends on the expectation and trust that Digital Assets can be used for future payment transactions (see valuation section above). Among others, persistent high volatility, changes and advances in technology, fraud, theft and cyber-attacks and regulatory changes may prevent the establishment of Digital Assets potentially rendering them worthless.

Liquidity risk

a). The market capitalisation of the digital assets industry is mainly led by Bitcoin, which represents more than 50% of the total market capitalisation. A significant position in any digital asset other than Bitcoin (and, depending on the case, including Bitcoin) may require several days or weeks to be unwinded with a possible negative effect on the price of the Digital Asset.

b). The market for the relevant Digital Assets may experience periods of decreased liquidity or even periods of illiquidity, hence under certain market conditions, it may be difficult or impossible to liquidate a position.

c). There is no guarantee that a private company will conduct an initial public offering or provide an alternative exit strategy for your invested capital.

Technology risk

a). Technology relating to Digital Assets is still at an early stage and best practices are still being determined and implemented. Digital Assets technology is likely to undergo significant changes in the future. Technological advances in cryptography, code breaking or quantum computing etc, may pose a risk to the security of Digital Assets. In addition, alternative technologies could be established, making some Digital Assets less relevant or obsolete.

b). The functioning of Digital Assets relies on open-source software

(Non permissioned distributed ledger). Developers may introduce weaknesses and programming errors into the open-source software or may stop developing the open-source software (potentially at a critical stage where a security update is required), keeping Digital Assets exposed to weaknesses, programming errors and threats of fraud, theft and cyber-attacks (see also ″Fraud, theft and cyber-attack risk″ below).

Some Digital Assets networks have experienced a surge in the number of transactions over the last few years. An increasing number of transactions coupled with the inability to implement changes to Digital Assets technology may result in a slower processing time of Digital Assets transactions (potentially days to verify a transaction) and/or a substantial increase in Digital Assets transaction fees paid to so called ″miners″ (when relevant) for facilitating the processing of transactions.

- Base layer transactions on a DLT or other distributed ledger are irreversible and final, and the history of transactions is computationally impractical to modify. Consequently, if the Client initiates or requests a transfer of Digital Assets using an incorrect distributed ledger address, it will be impossible to identify the recipient and reverse the defective transaction.
- The Client should be aware that any purchase and sale of Digital Assets may be stored in a public distributed ledger and may therefore be visible to the public. Such decentralised public ledger is neither a property of nor under control of Taurus. Information available on the decentralised public ledger may be exploited or misused in unforeseen ways.

Hard fork risk

a). Since there is no central body (e.g. a central bank or a government agency) overseeing the development of technology relating to Digital Assets, the functioning of Digital Assets, as well as further improvements of such functioning (e.g. ability to increase number of transactions, reduce processing time, reduce transaction fees, implement security updates), relies on the collaboration and consensus of various stakeholders, among others, developers enhancing the open-source software related to a Digital Asset or so called ″miners″ facilitating the processing of transactions. Any disagreement among stakeholders may result in a split of the Digital Asset network into two or more incompatible versions (such an event called a ″hard fork″).

b). As a result, trading venues on which Digital Assets are traded may suspend (temporarily or indefinitely) the ability to trade a particular version of a Digital Asset. Consequently, the Investors in the Digital Asset may (i) not get exposure (indefinitely) to all versions following a hard fork and forego the value of one or more versions, or (ii) may get exposure to a version on a delayed basis (in which case that version might have lost a significant part or all of its value).

c). In addition, hard forks may result in instability of a Digital Asset version and hard forks or the threat of a potential hard fork may prevent the establishment of the corresponding Digital Asset as an accepted long-term medium of exchange.

Fraud, theft and cyber-attack risk

a). The particular characteristics of Digital Assets (e.g., only exist virtually on a computer network, transactions in Digital Assets are not reversible and are done anonymously) make it an attractive target for fraud, theft and cyber-attacks. Various tactics have been developed (or weaknesses identified) to steal Digital Assets or disrupt Digital Assets technology (to name a few: ″51% attack″ where an adversary may take control over Digital Assets technology by providing 51% of the computer power in the Digital Assets network or ″denial of service attack″ where an adversary attempts to make Digital Assets network resources unavailable by overwhelming it with service requests. This may result in significant waiting periods, network congestion and delays during which the Client may be precluded from disposing over the relevant Digital Assets while their value may fluctuate significantly, or which may otherwise result in loss or damages).

b). Investors in any particular Digital Asset are directly exposed to fraud, theft and cyber-attacks: (i) Any high profile losses as a result of such events (e.g. bankruptcy of the then largest Digital Assets exchange Mt. Gox in February 2014) may raise scepticism over the long-term future of Digital Assets and may prevent the establishment of Digital Assets as an accepted long-term medium of exchange and may increase the volatility and illiquidity of Digital Assets; (ii) any loss resulting from fraud, theft and cyber-attacks relating to hedging party(ies) of the Issuer will be borne by the Investors.

c). Digital Assets are subject to a higher risk than usual of market abuse, market manipulation and insider dealing by market participants, due to a lack of regulation, supervision, market control and/or liquidity.

Legal, tax and regulatory risks

a). Risk of non-compliance or change of legal and regulatory framework: The legal, tax and regulatory framework governing Digital Assets in and outside of Switzerland is far from settled and continuously evolving. Existing laws and regulations, changes to the legal, tax and regulatory framework and related measures by regulators or other governmental authorities may affect the compliant issuance, domestic and international tradability and transferability or convertibility of the Client's Digital Assets and may potentially result in a full or partial loss of units or reduction of value (including reduction to zero) thereof.

b). Any forthcoming regulatory actions may result in the illegality of some Digital Assets or the implementation of controls relating to the trading

(and therefore liquidity) of Digital Assets. In addition, control mechanisms may increase Digital Assets transaction fees significantly (and therefore affecting the bid/offer spread of the Product). Investors should ensure that investing in any Digital Asset complies with their local regulation.

Supervision risk

a). As of today, Digital Assets do not have a function as and/or the full characteristics of a legal tender (even if some Digital Assets may be accepted for payment in certain countries or jurisdictions by public institutions) and are currently not supervised by any authority or institution such as a central bank.

b). Consequently, there is no authority or institution which may intervene in the Digital Assets market to stabilize the value of Digital Assets or prevent, mitigate or counter-attack irrational price developments of Digital Assets.

Operational risk

a). Sending Digital Assets to an incorrect and/or a wrong distributed ledger address leads to a total and irremediable loss of funds. Once a transaction is executed, it is impossible to cancel or reverse this transaction. Therefore, users shall always check that a destination distributed ledger address is correct before to confirm a transaction.

Credit & counterparty risk

a). In the case of tokenized securities, the risk of default or bankruptcy of the underlying issuer is material in line with private equity and/or private debt investments.

Specific risks related to the custody of Digital Assets Among the digital assets class, the following points have to be outlined when it comes to custody of digital assets:

a). Owning a digital asset is equivalent to owning the private key (equivalent to a secret pin) that gives you access to it.

b). Losing this private key is equivalent to ever accessing those assets again. There is no central authority to contact to regenerate that key.

c). Having this private key stolen is equivalent to giving full access to the assets to the malicious person/entity.

It is therefore of utmost importance that client’s back-up these private keys and store them securely.

In summary, it is highly recommended to only invest in Digital Assets the amounts the Client can afford to lose.

6. Adequacy of investment in digital assets with financial objectives

Investors willing to have exposure to digital assets should ensure their profile matches with the below characteristics of the asset class. Investors should seek advice from their investment advisors if they have any questions on the appropriateness of their profiles with the investment in digital assets, as well as to enhance their successful selection of opportunities within the asset class, according to their financial objectives and their risk tolerance.

Target clients	Private and Professional
Knowledge and experience	Intermediate and Expert
Ability to bear losses	Total loss of capital possible
	Not recommended to clients with no loss of capital possible.
	Total default or bankruptcy of Issuers possible.
Risk reward profile	High risk
Investment objective	Diversification
	General asset accumulation
	Growth
	Hedge against systemic risk
Investment horizon	Short term (for speculation purpose only)
	Medium to long term

Please contact the following person should you have any questions:

GUIDE ON RISK MANAGEMENT

Mr. Joshua Tari

Manager, Supervision Department

Email: tjoshua@vfsc.vu

Phone: (678) 22247

Fax: (678) 22242

Dated this 28 day of September 2021