VASP Policy Manual

Twofish Enterprises (Asia) Limited

June 22, 2023

Contents

1 Introduction **5**

1.1 History . . . 5

1.2 The External Assessor Review process . . . 6

1.3 Schedule . . . 7

1.4 Organization . . . 7

1.5 Public comment and review . . . 8

1.6 Waivers and modifications . . . 8

1.7 Contractual obligation . . . 8

2 Governance **9**

2.1 Objectives . . . 9

2.1.1 General objectives . . . 9

2.1.2 Specific objectives . . . 9

2.2 Stakeholders . . . 9

2.2.1 Clients . . . 9

2.2.2 Investors . . . 10

2.2.3 Society . . . 10

2.3 Role based management . . . 10

2.4 Consolidation of roles . . . 10

2.5 Separation of roles . . . 10
2.6 Departmental hierarchy . . . 10
2.6.1 Task force . . . 10
2.7 Governance of Twofish . . . 11

3 Risk Management 12

3.1 Risk is our business . . . 12
3.2 The risk management process . . . 12
3.2.1 Windup and social impact risk . . . 13
3.3 External risks . . . 13
3.3.1 Hacking risks . . . 13
3.3.2 Market risks . . . 14
3.3.3 Denial of service risks . . . 14
3.4 Internal risks . . . 14
3.4.1 Loss of key personnel . . . 14
3.4.2 Rogue senior manager . . . 14
3.4.3 Software failure . . . 14
3.4.4 Loss of critical data . . . 14
3.4.5 Growth risks . . . 14
3.5 Business risks . . . 14
3.5.1 Critical vendor risk . . . 14
3.5.2 Windup risks . . . 14

4 Operations 15

4.1 Account acceptance . . . 15
4.1.1 KYC . . . 15
4.1.2 Financial intermediaries . . . 15

4.1.3 No cross-exchange, vostro, nostro accounts . . . 16
4.1.4 No third party trading for non-FI accounts . . . 16
4.2 Deposit process . . . 16
4.3 Withdrawal process . . . 17
4.4 Trading rules . . . 17
4.4.1 No proprietary trading . . . 17
4.5 Asset Custody . . . 17
4.5.1 No trading of client funds . . . 17
4.5.2 Monitoring . . . 17
4.6 Suspicous activity procedure . . . 17
4.7 Market surveillance . . . 18
4.8 Client greivance process . . . 18
4.9 Wallet management . . . 18
4.9.1 Business operations wallet . . . 18
4.9.2 Hot wallets containing client funds . . . 19
4.9.3 Cold wallets containing client funds . . . 19
4.10 Cash and token management for bank-less exchanges . . . 19
4.10.1 No cash deposits by clients . . . 19
4.10.2 Paper cash must be physically separated . . . 19
4.11 Staff trading . . . 19
4.12 Staff side businesses . . . 20
4.13 Insurance . . . 20
5 Infrastructure **21**
5.1 Physical infrastructure . . . 21
5.1.1 Cash management (bankless) . . . 21
5.1.2 Petty cash . . . 21

5.1.3 Segreated cash . . . 21
5.1.4 Physically secure facility . . . 22
5.1.5 Cash management . . . 22
5.2 Cybersecurity . . . 22
5.2.1 Location of servers . . . 22
5.2.2 Administrative access . . . 22
5.3 Software deployment process . . . 23
5.3.1 Open Source only software . . . 23
5.3.2 Logs . . . 23
5.3.3 New version deployment . . . 23
5.3.4 Vendor patches . . . 23
5.3.5 Server reboot . . . 23
5.3.6 Security issues . . . 23
5.3.7 Backups . . . 23

6 Development and growth **24**

6.1 Token admission policy . . . 24

Chapter 1

Introduction

This operations and policy manual covers the design effectiveness of the Virtual Asset Trading Platform's proposed structure, governance, operations, systems and controls, with a focus on key areas such as governance and staffing, token admission, custody of virtual assets, KYC, AML/CFT, market surveillance, risk management, and cybersecurity.

The operations and policy manual will describe the design and rationale behind the policies and procedures for a virtual asset trading platform. Each chapter will contain an set of operational policies and standards as well as an evaluation section. This evaluation section will be reviewed by an external assessor to indicate compliance with the chapter in question.

1.1 History

This operations and policy manual arose out of the institution gap that arose from the institution of licensing for virtual asset service providers in Hong Kong by the Securities and Futures Commission. The primary objective of the SFC within Hong Kong is to protect the investing public through consumer protection and measures to insure license stability. As part of the application for licensing the SFC requires that an applicant prepare a Phase 1 External Assessor Report which is an assessment of the the virtual asset exchange, and once the applicant receives an approval in principal, the external assessor will prepare a report describing the implementation of the measures within the report.

However, this creates a dilemma in that neither the SFC or the external assessor is in a position to give a virtual asset service provider directions on what the provider should do. The job of the SFC to focus on outcomes and the SFC cannot and will not provide specific technical instructions on what a virtual asset service provider should do. The job of the external assessor is to audit and also to judge outcomes, but again, they are not in a position to design and implement a system.

Moreover, the mechanism of licensing decreases clarity and transparency, and increases cost. Without joint communication each virtual asset service provider may be redoing the same practices and expending duplication of resources. Furthermore, in the area of cybersecurity and technology, best practices suggest value in sharing information and increased public understanding and awareness over the internal processes of an exchange.

It is with this in mind that we have begun our licensing process by preparing this operations and policies manual and making it open to the public. Along side this manual are checklists and forms for external assessors where then can comparing existing infrastructure to best practices.

1.2 The External Assessor Review process

The external assessor review "EAR" process will begin with the development of a policy and procedures manual that will state best practices for the exchange. One the operations manual is completed the firm will under go a self-assessment by which the firm will find issues for improvement.

The phase one EAR report ("EAR1") and the self-assessment will then be given to a team of external assessors. The terms of reference for the assesors for the phase one report will consist of:

- Are the standard in place adequate for the exchange
- Has the self-assessment identified all of the outstanding issues and come up with a plan for action?
- Are the resources that have been allocated sufficient for the plan of action?

The EAR1 report will be given to the SFC as part of its licensing application. Once the SFC gives approval in principle, the firm will execute the play in the EAR1 report and the assessment team will review the progress of the firm for the EAR2 report.

1.3 Schedule

- 2023 July 15 - First draft of operations manual finished
- 2023 August 15 - Estimated date of completion of phase one report and initial submission to SFC
- 2024 Feburary 29 - Absolute deadling for submission of application to SFC
- 2024 June 1 - End of transitional period

1.4 Organization

This manual is organized into the following chapters

- Governance and Staffing - This will describe the governance structure and human resources of the firm
- Risk management - This section will describe the risk management process and the specific risks that have been identified for the firm.
- Operations - This will describe the operations of the business. This section will include KYC procedures
- Infrastructure - This chapter will describe the technical infrastructure of the firm. Included in this section are the cybersecurity and custody arrangements
- Development and growth. This section will describe the considerations to be undertaken as the company grows and develops. Included in this section will be token admission policies.

1.5 Public comment and review

The operations manual for the exchange is a living document will be made public, and the public in general and clients of the firm will be encouraged to propose suggestions for improvement.

1.6 Waivers and modifications

The operations manual will be reviewed by senior management with public input at least one per year. In addition, the managing director may modify the terms of the operations manual by placing a notice in writing.

The instructions of the operation are standing instructions, however in the event that it is necessary to protect the interests of the clients or other stakeholders, a waiver to the instructions in the manual may be presented.

1.7 Contractual obligation

Nothing in this manual shall establish a contractual obligation with any outside parties. However, the contents of the manual are intended to be considered for fitness for licensure by the regulator.

Chapter 2

Governance

2.1 Objectives

2.1.1 General objectives

2.1.2 Specific objectives

2.2 Stakeholders

Stakeholders are

2.2.1 Clients

The key stakeholders in the firm are the clients who have entrusted their money into the firm. In contrast to many industries where the client can be seen merely as a means for the firm to generate revenue

2.2.2 Investors

2.2.3 Society

2.3 Role based management

2.4 Consolidation of roles

2.5 Separation of roles

2.6 Departmental hierarchy

2.6.1 Task force

2.7 Governance of Twofish

As a research laboratory, the organizational structure of Twofish is designed to resemble that of university research laboratory than that of a commericial business. In particular, in order to rapidly conduct research, the staff of the laboratory will consist of a principal investigator and co-investigators.

We propose that the "external assessors" team that is assesses the fitness of Twofish be made a permanent body with a direct reporting line to audit and compliance functions. There will be a non-executive chairman which will monitor the financials and operations of the PI and co-PI's, and also monitor financial risk and impact of the research program to the wider community.

Chapter 3

Risk Management

Risk is our business - James T. Kirk (Return to Tomorrow)

3.1 Risk is our business

The firm as placed as the front the chapter on risk management. Risk is unavoidable and is essential for the type of technological and social progress that the firm seeks. The goal of the firm is not to avoid risk, but to manage risk and embrace risk. Through financial technology our firm intended to transfer from those who are unable or unwilling to bare risk to those who are able and willing to assume risk in exchange for additional reward.

3.2 The risk management process

The risk management process consists of five steps

- Identify risks
- Analyze risks
- Prioritize risks

- Mitigate risks
- Monitor risks

Risks should not be seen in isolation but holistically. Extreme care should be taking to insure that risks are reduced and properly transfered and that risk are not simply ignored or passed on to persons or socialized.

This chapter of the policy management should be reviewed each quarter by senior management in order to identify and prioritize each risk. Analysis of risk should include not only impact on the firm but also risks to financial stability.

3.2.1 Windup and social impact risk

Risks should include not only impact to the firm but also risk to clients that result from a voluntary or involuntary liquidation. In case of a windup, the firm should be set up to be able to exit the market with minimial disruption to clients and the overall market.

3.3 External risks

3.3.1 Hacking risks

Mitigations

- minimize the amounts of assets under custody
- have mechanisms for rapid detection of suspicious activity
- have the ability to have an emergency shutdown
- keep clear audit trails

3.3.2 Market risks

The main mechanism by which the firm will deal with market risk is not to have mismatched liabilities and assets. Any client funds held should be held in the same tokens that the liabilities are created in and should not be exchanged for other tokens.

3.3.3 Denial of service risks

3.4 Internal risks

3.4.1 Loss of key personnel

3.4.2 Rogue senior manager

3.4.3 Software failure

3.4.4 Loss of critical data

Action item - insure that backups are done and perform quarterly tests to insure that backups are recoverable

3.4.5 Growth risks

3.5 Business risks

3.5.1 Critical vendor risk

3.5.2 Windup risks

One key risk is what happens to the market and the clients in the event of either a voluntary or involuntary windup. It is possible that business objectives will change, and in case of a windup, it is the responsiblity of the firm to insure that this is done with minimial disruption and that all creditors are quickly and promptly paid.

Chapter 4

Operations

4.1 Account acceptance

The types of accounts that we expect to open can be classified as:

- Retail accounts
- Corporate accounts
- Financial intermediaries
- Staff accounts

Our main clients are expected

4.1.1 KYC

4.1.2 Financial intermediaries

We consider licensed financial intermediaries including money services operators, family offices, and license brokers to be low risk, provided that they are licensed in a reputable jurisdiction such as Hong Kong, Singapore, and Dubai. It is our expectation that a licensed financial intermediary would maintain adequate

AML/KYC protections to satisfy their regulators and hence it would be unnecessary for us to add an additional level of AML/KYC.

Our main concern regarding due dilligence regarding financial intermediaries is that they are who they say they are, and that they the information that the provide is accurate. In onboarding a financial intermediary, the staff will check to see that the intermediary is in fact licensed and that the person opening the account is an authorized agent of the intermediary. The staff will monitor the intermediary with ongoing checks to make sure that there has been no enforcement action taken.

4.1.3 No cross-exchange, vostro, nostro accounts

The company will not maintain an account with another exchange nor allow another exchange to hold an account with the company, and will not maintain nostro or vostro accounts. Our main concern is that cross exchange accounts will create "hidden leverage" in the financial system and will cause leverage

4.1.4 No third party trading for non-FI accounts

Persons who are not financial intermediaries are not permitted to trade on the exchange on behalf of third parties.

4.2 Deposit process

The deposit process consists of the user sending tokens into the deposit wallet, and then the system moving tokens from the deposit wallet into the accumulator wallet. The trading system will generate the keys of the deposit wallets, and these keys are stored encrypted in the database.

The private keys of the accumultator wallet are available only with the a senior manager, and should not be stored on the trading platform. Copies of the private keys of the accumulator should be stored split in two and stored in the archvial location.

4.3 Withdrawal process

The withdrawal process consists of several steps.

- Funds are moved from the cold wallets to the hot wallets and made available for withdrawal. Typically this transfer should be made once per day and should consist of 120 percent of the average expected delay withdrawal volume.
- Withdrawals are approved by a staff member
- Withdrawals are then queued by the hot wallet and approve by a manager

4.4 Trading rules

4.4.1 No proprietary trading

The firm is strictly prohibited from using its own capital or client funds to trade on the exchange.

4.5 Asset Custody

4.5.1 No trading of client funds

All client funds must be held in the same form that was deposited by the client. The firm is strictly prohibited from using client funds for the purpose of trading.

4.5.2 Monitoring

The following daily reports should be compiled and made available to the customer advocate.

4.6 Suspicous activity procedure

Staff will be trained to encourage a compliance culture with the following process

- Staff will be given compliance training as to how to identify and handle suspicious trading activity. Staff will also be given compliance training concerning "anti-tipping" procedures and that any suspicious activity should not be raised with the client.
- In case, staff believes that there is a compliance issue that can be addressed by senior management then will be a hotline that will allow the staff to raise the issue with compliance
- Staff will also be given training on how to raise an issue with the financial regulators or law enforcement in case they believe that the issue cannot be resolved within the firm. Staff will be given training as to their legal rights and obligations.

4.7 Market surveillance

As the exchange will not be trading proprietary tokens and tokens will be traded on a different market, we do not

4.8 Client greivance process

4.9 Wallet management

All wallets should be inventoried and each wallet should be desginated as a business wallet, a client funds wallet.

All business wallets and client funds wallets should be held on separate devices. All devices with client wallets should contain only corporate information.

4.9.1 Business operations wallet

* A wallet for business operations can contain up to 250k HKD using a software device in the form of a mobile device. This mobile device is the property of the company and should not contain any

4.9.2 Hot wallets containing client funds

4.9.3 Cold wallets containing client funds

4.10 Cash and token management for bank-less exchanges

4.10.1 No cash deposits by clients

The exchange will not hold any cash by clients or accept any cash deposits. All paper fiat held by the company are intended for internal business purposes only.

4.10.2 Paper cash must be physically separated

All paper cash held by the firm must be held in a secure location and kept strictly separate from other cash, particularly any person cash held by staff. All deposits and withdrawals of cash from the firm must be records in the ledger.

The company will maintain an inventory of all locations which firm cash is being kept and will insure that adequate security standards. See physical infrastructure.

4.11 Staff trading

We encourage staff to trade on our systems in the belief that having our staff use our one products and services will improve them. However we will maintain the following principles and policies to maintain protection with the wider financial community

- Staff must provide a written statement as to the nature of their trading
- Staff are only allowed to trade liquid tokens for which the firm does not maintain a proprietary interest
- Orders by staff can only be executed using personal funds

- Orders by staff will be made only through the standard trading interfaces. Staff are strictly prohibited from given staff privileged trading over non-staff accounts.
- Staff must sign a waiver stating that in case of loss or liquidation of the company, that all liabilities to staff will be paid out only when liabilities to other clients are paid out in full. Staff must also sign a two year "clawback" provision by which any profits made by personal trading are subject to "clawback" in case the firm folds

4.12 Staff side businesses

We encourage staff to have side businesses and other crypto related businesses. However, staff must report any side businesses which may create a conflict of interest to senior management.

4.13 Insurance

Need to get price quotes for D&O and liability insurance

Chapter 5

Infrastructure

5.1 Physical infrastructure

5.1.1 Cash management (bankless)

* All corporate cash must be physically segregated from none personal cash

  * All movement of corporate funds into an out of physical cash must be recorded

  * Physical cash is used only for corporate operations. Twofish will not handle physical cash for clients.

  * The location of all cash must be physically inventoried

5.1.2 Petty cash

* The company may hold up to HKD 20k in non-secure facilities and in form of petty cash.

5.1.3 Segreated cash

* Amounts up to HKD 200k may be held in a safe in a non-secure location.

5.1.4 Physically secure facility

* Amounts over HKD 200K must be held in a physically separate secure location.

5.1.5 Cash management

* The company should hold two weeks operational reserve in the form of paper fiat.

* The company should hold the remaining in the form of two

* The company should at all times have at least two contacts that can convert paper cash to and from virtual assets

5.2 Cybersecurity

5.2.1 Location of servers

The location of the servers will be reported to the

5.2.2 Administrative access

Administrative access is allowed only for devops work. No trading is allowed outside of the standard trading interfaces.

- The location of the exchange server is hidden behind a load balancer or cloud server. The IP address of to allow access is not publically available

- Direct root access to the server is not allowed, and shell access to the exchange server is only through passwordless tokens

- (TODO) There should be a two step login process by which the user logs in first to a proxy server, and then from the proxy server undertakes a second login to the exchange server

5.3 Software deployment process

5.3.1 Open Source only software

The firm has a policy of only running open source software. All software which is run on productions backend services is publically available via the github repository for the company.

5.3.2 Logs

The technology department should maintain a log of incidents and events.

5.3.3 New version deployment

The process for deploying a new version of OpenCEX:

- New code deployments should generally be done on the weekend
- Deployments must be signed off by the chief technology officer or his delegate
- The deployment officer will examine the source code and verify that it is the correct version
- Code is downloaded from OpenCEX main site and merged with local changes on github
- Code is deployed on test server and run for two to three days.
- Before there is a server upgrade the directory containing the server engine will be backed up
- When there are no anomalies the code will upgraded on the production server

5.3.4 Vendor patches

The servers are operating under Linux Ubuntu. Vendor upgrades should be made as soon as possible but in no event more than one week after the vendor upgrade is released.

5.3.5 Server reboot

The server should be reboot from a cold start at least once a week.

5.3.6 Security issues

The firm will work closely with vendors to identify and close security issues. Security related bugs will be addressed through standard “responsible” disclosure mechanism.

5.3.7 Backups

Chapter 6

Development and growth

6.1 Token admission policy

Tokens will be added onto the exchange only upon the recommendation of an independent token admission board. This exchange will work with other exchanges to insure that any new tokens are issued simulatenously on several exchanges.

We shall inform the Securities and Futures Commission if we are considering any new tokens under consideration.

We will work with other exchanges and regulators to develop standards for the issuance of new tokens, particularly tokens of a securities nature. We will not require tokens to sign any exclusive listing tokens. Our fees for issuing tokens will be limited to the administrative costs of adding new tokens and we will not turn token listing into a profit center.