Risk Assessment

CONTENTS

1. SUMMARY

Gilgamesh Financial Services and/or GFX Securities and/or the Company recognizes its obligation to ensure the protection of client funds and adherence to local and international regulations. This policy was created to ensure full/continual compliance and licensing with the Mauritius Financial Services Commission (MFSC) and international best practice.

This Risk Assessment Report, in conjunction with all other internal policies, assesses the use of resources and controls to eliminate, mitigate and/or manage vulnerabilities that are exploitable by threats internal and external to Gilgamesh Financial Services and/or GFX Securities and/or the Company.

The scope of this risk assessment effort was broadly defined and intended to outline and document the adequacy of the management, operational and technical security and risk mitigation controls that are currently in place to secure the operations of Gilgamesh Financial Services and/or GFX Securities and/or the Company. These requirements address security controls in the areas of computer hardware and software, data, operations, administration, management, information, facility, communication, personnel, and contingency.

The methodology used to conduct this risk assessment is qualitative, and no attempt was made to determine any annual loss expectancies, asset cost projections, or cost-effectiveness of security safeguard recommendations.

The risk assessment of Gilgamesh Financial Services and/or GFX Securities and/or the Company identified no major vulnerabilities in the areas of Management, Operational and Technical Security.

All other minor vulnerabilities are adequately addressed in existing policies and are well within manageable levels.

2. INTRODUCTION

The purpose of this risk assessment is to outline and document the adequacy of the management, operational and technical security and risk mitigation controls that are currently in place to secure the operations of Gilgamesh Financial Services and/or GFX Securities and/or the Company. This risk assessment provides a structured

qualitative assessment of the operational environment. It addresses sensitivity, threats, vulnerabilities, risks and safeguards.

SCOPE

The scope of this risk assessment assessed the adequacy of the management, operational and technical security and risk mitigation controls that are in place (implemented or planned) to secure the operations of Gilgamesh Financial Services and/or GFX Securities and/or the Company and to eliminate and/or manage vulnerabilities exploitable by threats internal and external to the Company. If exploited, these vulnerabilities could result in:

- Operational Risk - the risk of a break in operational continuity
- Compliance Risk - the risk of violating local or international laws/regulations
- Customer Risk - the risk of customers exploiting the business platform to commit a crime
- Employee Risk - the risk of high-risk behaviour, whether inadvertent, negligent or malicious
- Information Risk - the risk of sensitive data not being protected

Any recommended safeguards will allow management to make decisions about risk mitigation initiatives. This assessment excludes risks accepted by the customers of the client.

USE OF DATA

The Company may process Personal Data of a customer on the following bases and for the following purposes:

To carry out obligations arising from any agreements between a customer and the Company.

For notifications about changes of products and/or services, as well as other important alterations affecting performance of an agreement between a customer and the Company.

For notifications about products and/or services of a Company. A customer must give his/her explicit consent to receive such information.

If the Customer is asked to provide Personal Data to comply with legal requirement or to conclude an agreement between the Customer and the Company, the Company shall make it evident and advise the Customer regarding the purpose of collection of Personal Data.

3. PHILOSOPHY

The assessment is broad in scope and evaluates vulnerabilities affecting operations, management, and technical aspects related to the business. The assessment may recommend appropriate safeguards, thereby permitting management to make knowledge-based decisions about risk mitigation initiatives. The methodology addresses the following types of controls:

Management Controls: Management of the information technology (IT) system and the management and acceptance of risk

Operational Controls: Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls

Technical Controls: Hardware and software controls providing automated protection to the system or applications (Technical controls operate within the technical system and applications.).

RISK ASSESSMENT PROCESS

This section details the risk assessment process performed during this effort. The process is divided into pre-assessment, assessment, and post-assessment phases.

The significance or weight of a risk factor within a business relationship or an occasional transaction will, generally, rely on the context of the specific relationship or transaction. The Company has established a risk-scoring system based on which the extent of ML/FT risk of a prospective customer or already established customer shall be determined. The individual risk factors (the “Variables”) are weighted based on a scoring system, with scores assigned from 1-10 to the individual risk factors depending on the perceived severity thereof: a score of 1 is awarded to the Variable which poses the lowest risk and a score of 10 is awarded to the Variable which poses the highest risk. The higher the risk weighting, the higher the level of CDD that must be carried out for such customer.

The rating and weighting for each variable are interlinked. The risk rating according to the perceived level of ML/FT risk adopted by the Company for business relationships are classified as low, medium, high risk. The Client risk matrix can be located within our Internal Procedures & Client Risk Matrix Policy. PRE-ASSESSMENT
The Customer assumes full responsibility for the safekeeping of information received from the Company and shall bear the risk of any financial loss caused by unauthorized access to the Customer's trading account by any person. The Customer is responsible for keeping all login details safe. The Company strongly recommends that user details are not written down or saved.

All losses caused by Force Majeure event shall be exempt from the responsibility of the Company.

The Customer shall bear all financial and other risks when completing operations (or actions connected with these operations) on financial markets that are statutorily prohibited or restricted by the legislation of the jurisdiction in which the Customer is resident. The Customer must be aware of such legislation and check whether there are any restrictions before initiating trading.

The Customer must familiarize themselves with commission and other charges of the Company before trading. If there is any doubt, the customer should first contact customer support.

ASSESSMENT

Step 1: Document Review

The assessment phase began with the review of documents and policies provided by the members of the Gilgamesh Financial Services and/or GFX Securities and/or the Company team. Detailed interviews allowed completion of a questionnaire and identification of potential threats.

Step 2: System Characterization

In this step, the analyst defined the boundaries of the IT systems, along with the resources that constitute the system, its connectivity, and any other elements necessary to describe the system. Dependencies were clarified. Sensitivity of the system and data was discussed in the final section of the characterization.

Step 3: Vulnerability Identification

In this step, the risk assessment team developed a list of potential vulnerabilities that could be exploited.

Step 4: Risk Determination (Calculation/Valuation)

In this step, the risk assessment team determined the degree of risk to the operations of Gilgamesh Financial Services and/or GFX Securities and/or the Company. In some cases, a series of vulnerabilities could combine to create the risk. In other cases, a single vulnerability could create the risk. The determination of risk for a particular threat source was expressed as a function of the following:

Likelihood Determination: The following governing factors were considered when calculating the likelihood of the probability that a potential vulnerability might be exploited in the context of the associated threat environment:

- Threat source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

Level	Likelihood Definition
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede the vulnerability from being exercised.

The following table defines the likelihood determinations.

Impact Analysis: The next major step in measuring level of risk was to determine the adverse impact resulting from successful exploitation of a potential vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the operational, management or technical stability of Gilgamesh Financial Services and/or GFX Securities and/or the Company.

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission, reputation, or interest.

	Risk Level Definition
High	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Moderate	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	The Authorizing Official must determine whether corrective actions are still required or decide to accept the risk.

Risk Determination: The following table provides a definition for the risk levels. These levels represent the degree or level of risk to which a system, facility, or procedure might be exposed if a given vulnerability were exercised:

Step 5: Risk Mitigation Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, were provided. The goal of the recommended controls is to reduce the level of risk to an acceptable level. The risk assessment team considered the following factors when recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options
- Legislation and regulations
- Organizational policy
- Operational Impact
- Safety and reliability
- Sensitivity of the data and the system

The recommendations were the results of the risk assessment process and provide a basis by which the Gilgamesh Financial Services and/or GFX Securities and/or the Company can evaluate and prioritize controls.

POST ASSESSMENT

Step 1: Risk Mitigation

Because the elimination of all risk is usually impractical, senior management and business stewards should assess control recommendations, determine the acceptable level of residual risk, and implement those mitigations with the most appropriate, effective, and highest payback.

Step 2: Ongoing Monitoring & Periodic Review

The agreed-upon milestones to mitigate the risks are reportable to the Senior Management of Gilgamesh Financial Services and/or GFX Securities and/or the Company and must be reviewed periodically.

Once a business relationship is established, the Company will ensure that the customer is constantly monitored. Ongoing monitoring may be divided into 2 elements:

A. Keeping information, documents and data held on the customer up-to-date;

The Company will ensure that information, documents or data relative to the customer, as well as any assessment thereof, remain up-to-date and relevant. Files will be reviewed periodically, in line with the applicable regulations and this Manual. Updating can be carried out through one or a combination of methods. The following methods are used by the Company:

I. Trigger events

The Company's systems would detect when documents with an expiry date would need to be updated. This trigger event would alert the MLRO to carry out another screening on the customer and obtain new unexpired documentation from the customer.

II. Periodic Reviews

Depending on the level of risk, the Company' systems will set up a schedule to: review the customer file to see if it needs adjusting/updating; carry out another screening on the customer; check if the business relationship remains within the risk appetite of the Company; and ensure a STR in relation to a customer does not need to be filed with the Authorities. The Company's periodic review schedule is listed below:

Customer Rating	**Refresh**
Low	Every 3 years
Medium	Every 2 years
High	Every 1 year

B. Scrutiny of Transactions

Transaction monitoring involves scrutinizing transactions undertaken in the course of a business relationship to ensure that these are consistent with the Company's knowledge of the customer's risk profile. An unusual transaction should serve as a red flag or a trigger event, whereby the Company would need to assess the situation in question and establish whether:

i. the transaction is suspicious and ought to be reported to the Authorities; or ii. The business relationship remains within the risk appetite of the Company; iii. There are material changes in the activity carried out by the customer, in which case the assessment will be updated, the customer screened, and if necessary, the CDD information and documentation is changed, updated or enhanced.

The Company's automated systems maintain an audit trail of the alerts raised and permit the creation of a report demonstrating the reasons why an alert was raised, and which rules or parameters were considered when conducting transaction monitoring in the below 2 ways:

i. In real time [Pre-Transaction Monitoring ("Pre-TM")], whereby transactions or activities are reviewed as they take place or prior to finalization;

ii. After the event [Post-Transaction Monitoring ("Post-TM")], where transactions and patterns are reviewed after execution.

The following is a (non-exhaustive) list of factors which the Company's automated systems apply to detect transactions that are unusual:

i. a significant change in the value of a series of transactions or in the overall volume or frequency of transaction (Post-TM);

ii. A significant change in the value of an individual transaction (PreTM); iii. unusually large transaction/s (Pre-TM / Post-TM);

iv. the immediate repetitive deposit and withdrawal in rapid succession of funds on an account (Post-TM);

v. a change in the geographical destination or origin (or other form of connection) of a transaction (Post-TM);

vi. mismatch between jurisdictional connections as determined through the business and risk profile (Post-TM);

vii. mismatch between customer's risk profile and value and/or level of transactions (Pre-TM);

viii. request for information received from the FIAU or the police on a customer's transactions (Pre-TM/Post-TM;

ix. identify customers whose predominant source of funds are derived from digital currency exchanges and third-party payment processes that provide anonymity to the source of funds (Post-TM);

x. identify the customer undertaking multiple transactions

Concurrently of varying amounts and in different currencies (PostTM); and

I. identify instances where account holders have multiple private wallets and frequent changes are made corroborate the information in the system (post-TM);

II. identify customers attempting to obfuscate the movement, source or destination of funds such as by using digital currency mixers/tumblers (post-TM); and

xi. There are circumstances in which the licensee is able to determine as much on the basis of information in the Company's possession (e.g. geo-location information, IP address data, funding method data, etc.) with the information contained in the documents provided by the customer (Post-TM).

The above listed detection rules implemented by the Company's automated systems will be tested and fine-tuned by the Company and MLRO at least on an annual basis to ensure that whilst transactions and patterns are actually being detected, they are not generating too many false positives. Similarly, the above detection rules might need to be updated to reflect changing trends.

The Company, when assessing unusual transactions, will request from the customer information and/or documentation on one or a combination of the following:

i. The source of funds of that transaction;

ii. Any new operational activities;

iii. Any significant relevant changes relating to the customer, such as a change in occupation; and

iv. Any other information/documentation that the Company deems reasonably necessary to be satisfied that the funds are derived from legitimate sources.

Where notwithstanding the information and/or documentation received, the MLRO is not satisfied with the explanations provided or has doubts as to the veracity of the information/documentation provided, the MLRO will consider whether there are sufficient grounds to file a STR.

4. BUSINESS CHARACTERISATION

BUSINESS DESCRIPTION

Gilgamesh Financial Services and/or GFX Securities and/or the Company is the name of the legal entity incorporated in Mauritius. At the moment, Gilgamesh Financial Services and/or GFX Securities and/or the Company is in the position of an applicant for a Full Investment Dealer License (excluding Underwriting) that is granted by the Financial Services Commission of Mauritius (MFSC).

TRADING PLATFORM DESCRIPTION

Gilgamesh Financial Services and/or GFX Securities and/or the Company will obtain a White Label, after which the Company will be able to offer the MetaTrader 5 platform to its customers.

The software is licensed to foreign exchange brokers like Gilgamesh Financial Services and/or GFX Securities and/or the Company, who provide the software to their

clients. The software consists of both a client and server component. The server component is run by the broker and the client software is provided to the broker's customers, who use it to see live streaming prices and charts, to place orders, and to manage their accounts.

BUSINESS DEPENDENCIES

- Server(s)
- Bridge
- CRM
- Web Connectivity
- Portal Providers

INFORMATION SENSITIVITY

This section provides a description of the types of information handled by GFX Investment Group Limited and an analysis of the sensitivity of the information. The sensitivity of the information stored within, processed by or transmitted by GFX Investment Group Limited provides a basis for the value of the system and is one of the major factors in risk management.

Three potential impact levels (Low, Moderate, and High) are established for each of the information security objectives (confidentiality, integrity, and availability). The impact levels focus on the potential impact and magnitude of harm that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals.

During its onboarding, document collection and storage phases, the security of business and customer sensitive information was tested and found to be compliant in terms of international best practice when measured against confidentiality, integrity and availability requirements.

5. POLICY TESTING

During the risk assessment of Gilgamesh Financial Services and/or GFX Securities and/or the Company all related policies were inspected and tested against local regulations and international best practice. All policies were found to be adequate in

addressing the full spectrum of risks associated to the business and drafted in accordance with applicable legislatures.
These policies include:

- Anti-Money Laundering and Counter-Terrorism Financing Policy / KYC Policy
- Suspicious Reporting Policy
- Sanctions Policy
- Records Management Policy
- Employee Manuals
- Disaster Recovery Plan
- Order execution Policy
- Complaint Handling Policy
- Privacy Policy (with having EU GDPR as a milestone)
- Risk Disclosure

6. SERVICE / PRODUCT RISK ASSESSMENT

GFX Investment Group Limited recognises the risks of it being used for money laundering or terrorist financing derive from the products and services that it offers. The purpose of the Product Risk Assessment is to assess the level of Money Laundering or Terrorist Financing Risk posed by the product or service offerings of the business and then to document the mitigation elements thereof.

In accordance with the Companies AML/CFT Programme Policy, the Company adopts a risk-based approach to managing its money laundering and terrorist financing risks. Such an approach is essential to the effective allocation of resource to areas of highest risk and to the implementation of systems and controls that are proportionate to the risks and appropriate to the nature, scale and complexity of the operations.

Gilgamesh Financial Services and/or GFX Securities and/or the Company business is based exclusively on the provision of CFD transactions with customers. Hence the product risk remains constant for all customers and the business and is built into the

Customer Risk Assessment methodology of the Company. The product/service itself is considered to pose a low risk of money laundering for the following reasons:

- the limited ability to receive and make payments to third parties;
- the traceable nature of transactions;
- the potential volatility in value of the product/service;
- the lack of anonymity of the product/service;
- the product/service cannot be purchased with cash.

In its 2009 report titled “Money Laundering and Terrorist Financing in the securities sector” the FATF outlined the following vulnerabilities associated with CFD market access:

1. The number of firms offering the service has increased and can have substantial transaction volumes. These high transaction volumes can create a “Black Box” and increases the difficulty for financial institutions to understand transactions occurring in the account.
2. Non-face-to-face onboarding increases the risk of a firm not adequately identifying its customers.

Both points 1 and 2 have been mitigated by the Company by ensuring that adequate transactional monitoring software is employed and that all customers are adequately screened and vetted before they are accepted as clients of the Company

After taking account of all these factors and industry experience, the product/service risk is assigned an overall risk rating of Low and any risk emanating from this segment has been adequately mitigated by the Company.

7. COUNTRY RISK ASSESSMENT

GFX Investment Group Limited recognises the risks of it being used for money laundering or terrorist financing derive primarily from the jurisdictions in which it operates.

The Company has developed its own AML Country Risk Matrix approach which ranks the money laundering risk of a particular country according to where it appears on a number of indices, including UN sanctions lists, FATF Country Risk and more.
The purpose of the AML Country Risk Matrix is to assess the level of Money Laundering or Terrorist Financing Risk posed by a particular country and allows the business to set strict parameters for which countries it accepts. The AML Country Risk Matrix groups countries into the following categories, with associated rules applied:

Status	Rule	Example
Blacklisted	May not accept clients from these countries (override customer risk rating)	Sudan
High Risk	Apply Enhanced Due Diligence for clients from these countries	Ghana
Medium Risk	Apply Standard Due Diligence for clients from these countries (Only IF overall customer risk rating is also Medium)	Angola
Low Risk	Apply Simplified Due Diligence for clients from these countries (Only IF overall customer risk rating is also Low)	UK

The country of residence and the nationality of a prospective customer plays a significant part in a customer's overall AML risk rating. Customers from Blacklisted countries will be prevented from opening and or operating accounts with the Company.

After taking account of all these factors and industry experience, the country risk is assigned an overall risk rating of Moderate but is more than adequately mitigated by the employment of the Companies AML Country Risk Matrix.

8. RISKS ACCEPTED BY CUSTOMERS

There is an inherent amount of risk, which must be accepted by the customers of GFX Investment Group Limited. The business clearly expresses these risks to each customer and the below should be viewed as a brief outline of these risks.

RISK STATEMENTS

Online trading involves significant risks, as indicated hereunder. Prospective Customers should be aware that they can benefit as well as lose all or part of their funds when engaging in trading activities.

In making a decision to trade in the Company's products, Customers must rely on their own examination of the products, including the merits and risks involved. The Company does not provide advice of any kind, including tax, investment or legal advice other than general consultations to Customers. The Customer should not risk more than what he is prepared to lose. The Customer must ensure that he understands the risks involved and take into account his level of experience before deciding to trade Independent advice and consultation must be sought if the Customer deems it necessary.

Online trading involves a high degree of risk. Customers may not receive the amount that they initially invested due to any of these risks and may lose all or part of their funds.

EFFECT OF LEVERAGE

When executing trading operations under margin trading conditions even small market movements may have a great impact on a Customer’s Trading Account due to the effect of leverage. The Customer must take into consideration that if the trend on the market is against them, the Customer may sustain a total loss of their Initial Margin and any additional funds deposited to maintain Open Positions. The Customer shall be held fully responsible for all risks and resources used and the chosen trading strategy.

Majority of instruments are traded within wide ranges of intraday price movements. Consequently, Customers must carefully consider the fact that there is not only a high probability of profit, but also one of losses.

Majority of instruments are traded within wide ranges of intraday price movements. Consequently, Customers must carefully consider the fact that there is not only a high probability of profit, but also one of losses.

TRADING PLATFORM

The Customer shall assume the risk of any financial loss caused by the Customer either not receiving a notification from the Company or it being delayed.

The Customer acknowledges that unencrypted information transmitted by email is not protected from unauthorized access. The Customer also agrees that the Company shall have the right to delete messages sent to the Customer through internal mail 5 (Five) days after they have been sent, despite the fact that the Customer may not have received them yet.

The Customer assumes full responsibility for the safekeeping of information received from the Company and shall bear the risk of any financial loss caused by unauthorized access to the Customer's trading account by any person.

Customer shall bear all risks of financial loss caused by a Force Majeure Event.

The Customer shall bear all financial and other risks when completing operations (or actions connected with these operations) on financial markets that are statutorily prohibited or restricted by the legislation of the jurisdiction in which the Customer is resident.

The Customer must be aware of commissions and other charges before trading. Charges may be expressed in monetary terms, percentage terms or in other units of measurement and it is therefore the responsibility of the Customer to understand what such charges amount to.

RISK ASSESSMENT RESULTS

The table below represents the findings of an independent analysis into the operations, management and technical aspects of GFX Investment Group Limited.

Risk Vector	Likelihood	Impact	Risk Level	Mitigation

Operational Break	Low	High	Medium	Appropriately Mitigated: Risk Management Policy Deemed adequate
Management Failure	Low	Medium	Low	Appropriately Mitigated: Segregation of Duties
IT Break	Low	High	Low	Appropriately Mitigated: Global Servers
Legal Violation	Low	Medium	Low	Appropriately Mitigated: Internal and External legal counsel
Customer Exploit	Low	Medium	Low	Appropriately Mitigated: KYC Policy
Information Loss	Low	Medium	Low	Appropriately Mitigated: IT Policy/Backup Servers
Employee Dishonesty	Low	High	Medium	Appropriately Mitigated: Employee Screening/Segregation of Duties
Liquidity Risk	Low	High	Medium	Appropriately Mitigated: Only Liquidity Providers from G20 countries are used
Banking Risk	Low	Medium	Low	Appropriately Mitigated: Segregated accounts for clients funds/Only Licensed Banks will be used
Insurance Risk	Low	High	Medium	Appropriately Mitigated: Professional Indemnity insurance will be obtained for legislated sums

9. CONCLUSION

It is our finding that Gilgamesh Financial Services and/or GFX Securities and/or the Company has appropriately addressed and mitigated all identified operational, management and technical risks. The overall business risk is therefore classified as Low