Enjoy Optimal Trading with us.

OPTIM INVESTMENTS

OPTIM Investments

OPERATIONAL RISK MANAGEMENT POLICY

Updated: 12 October 2020

CONTENTS

Forward: This Policy document will define the relevant policies and governance to be followed by OPTIM Investments (the "Company") regarding the management of operational risk. The management of operational risk is an integrated part of the Company's overall risk management activities and it concerns all functions and personnel of the Company.

1. PURPOSE AND INTRODUCTION

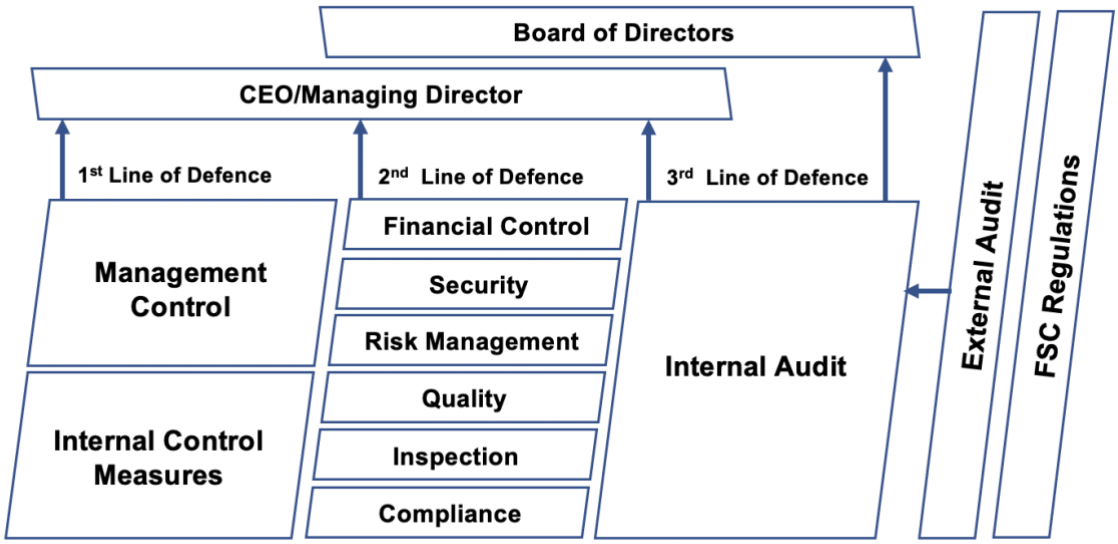
Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, including legal risk. It is inherent in every business organization and covers a wide range of issues. The Company manages operational risk through a control-based environment in which processes are documented and transactions are reconciled and monitored. This is supported by continuous monitoring of operational risk incidents to ensure that past failures are not repeated.

This Policy provides the strategic direction and guidelines on operational risk in order to ensure that an effective operational risk management and measurement process is adopted throughout the Company. The Policy also provides for the consistent and comprehensive capture of data elements needed to measure and verify the operational risk exposure, as well as to implement appropriate reporting systems and mitigation strategies.

Further to the above, the Company has in place controls and procedures in order to reduce the operational risk arising, as follows:

- Monitoring of the effectiveness of policies, procedures and controls;
- Use of systems to automate processes and controls to eliminate risk due to human error;
- Ongoing maintenance of procedures to prevent unauthorised actions and errors;
- Use of training to reduce the likelihood of human error arising from lack of expertise
- Maintaining a four-eye structure and implementing board oversight over strategic decisions made by the heads of departments;

The Company's operational risk management paradigm can be illustrated as follows:



This Policy outlines guidelines mandated by the Board of Directors in the identification, evaluation, measurement, monitoring and reporting of all operational risks associated with the activities conducted by the Company's organisation.

This Policy also describes the responsibilities of and requirements imposed upon the different functions of the Company to fulfil their operational risk management duties in order to maintain a safe and sound organisation.

It is recognised that operational risk cannot be confined to specific organisational units but remains largely the responsibility of line managers or owners of the core processes, and some defined and certain special and support functions (such as HR and Legal).

2. GENERAL APPROACH

The Company's operational risk management focuses on proactive measures in order to ensure business continuity as well as the accuracy of information used internally and reported externally, a competent and well-informed staff, and its adherence to established rules and procedures as well as on security arrangements to protect the physical and IT infrastructure of the Company.

3. ROLES AND RESPONSIBILITIES

3.1 Role of the Board of Directors

The Board of Directors is accountable for ensuring that the operational risks at the Company are adequately and effectively managed and has the responsibility for establishing a strong operational risk control environment and systems that fulfils the requirements of the laws of Mauritius, and is consistent with safe and sound business practices.

Consequently, the Board of Directors is responsible for adopting policy decisions concerning the operations of the Company and for the establishment and maintenance of adequate and functioning internal control mechanisms.

Exceptions to Operational Risk Management Policy, procedures and parameters established by the management will be reviewed and evaluated by the Board of Directors for appropriate resolution.

3.2 Role of the Chief Executive Officer

It is the CEO's responsibility, assisted by relevant advisory committee, to manage the risk profile of the Company. Consequently, it is the CEO's responsibility, assisted by relevant advisory committee, to develop and coordinate the operational risk management activities and systems across the Company and to ensure that the operational risk management as a whole is reviewed and updated when necessary.

3.3 Role of the Process Owners

Operational risk management is an on-going activity and an inseparable and integrated part of the Company's business operations and procedures. Therefore, while the Board of Directors is accountable for ensuring that the operational risks at the Company are adequately and effectively managed, the owners of processes and line managers, with possible operational risks, and those responsible for day- to-day operational risk management activities, are responsible for that the operational risk management policies and framework are secured and followed-up.

Each process (core and/or sub- process), is assigned an owner, who is responsible for monitoring and reporting risks on a regular basis, unless more urgent action is called for, and for ensuring that any material changes to and/or observations of the operational risk profile are recorded and fed into the business planning process.

3.4 Role of the Compliance Department

The Compliance Department is responsible for assessing compliance risk in relation to institutional matters such as governance, best practices and corporate social responsibility. The duties of the Department also include operational matters such as issues of reputation risk, and

matters of conduct such as conflict of interest, restrictions in trading with financial instruments, confidentiality, fraud and corruption including money laundering, prevention of terrorist financing and tax evasion. The Chief Compliance Officer reports to the Company's CEO and has direct access to the members of the Board of Directors.

4. PRINCIPLES FOR IDENTIFYING, ASSESSING, MONITORING AND MITIGATING OPERATIONAL RISK

4.1 General Principles

The Company identifies and assesses the operational risk inherent in all its material products, activities, processes and systems. Furthermore, the Company ensures that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures. The use of new products or systems should be approved in advance by the relevant internal body and the Compliance Department.

The Company mitigates operational risks by defining, documenting and updating the relevant business processes. Furthermore, the Company mitigates operational risk by following strict rules for the assignment of duties and responsibilities among and within the functions and a system of internal control and supervision. The main principle for organising work flows is to segregate the business-generating functions from the recording and monitoring functions. An important factor in operational risk mitigation is also the continuous development and upgrading of strategic information and communication systems.

4.2 Categorisation of operational risk

The Company has categorised the operational risk event types as follows:

i. **Internal Fraud:**
Risk resulting from dishonesty of personnel within the Company, such as forgery of documents, embezzlement, bribery, etc.

ii. **External Fraud:**
Risk resulting from dishonesty of individuals outside the Company that causes damage to the Company, such as forgery of financial documents, fraud, etc.

iii. **Clients, Products and Business Practices:**
Risk resulting from business practice, the introduction of a product, and the accessing of a customer's information that is inappropriate or noncompliant with regulations or rules, such as unauthorized transactions, unapproved dealings, money laundering activities, or the misuse of confidential customer information, etc.

iv. **Business Disruption and System Failures:**

Misuse of confidential customer information, etc. Risk resulting from anomalies in the system or the failure of the system in various other respects, such as inconsistency, disparity arising from combining operations, defects in the computer system or network system, or the usage of outdated or substandard technological tools.

This type of risk includes the following two sub-groups:

- Execution, Delivery and Process Management risks resulting from errors in methodology, in the operational process itself, or from employees within the Company and employees outside the Company. This type of risk includes: submitting inaccurate information, evaluating incorrect warranty values, failing to follow contract rules, a lack of knowledge and comprehension of employees in operations and usage of the computer system, inappropriate improvements in operations, and drawing incomprehensive contracts and legal documents that produce loopholes, etc.

- Damage to Physical Assets. This is the risk of property damage in the Company resulting from various accidents, such as conflagration, natural disasters, destruction of property, riots, political uprisings, terrorism, etc.

v. <u>Employment Practices and Workplace Safety:</u>

Risk resulting from the inappropriate hiring of employees, unjust compensation, or the mistreatment of employees, producing consequences such as litigation, resignation, or demonstration. Moreover, it includes risk stemming from the enforcement of safety regulations and the inability to control the environment in working conditions, causing detrimental effects on employees' health such as illness, or accidents while working.

4.3 Structure to identify and manage operational risks

The Company's activities and operations have been defined as a set of core and sub processes in which operational risks can occur, and in which the Company's operational risks consequently will be identified, reported, followed up and managed.

To reflect changes in the Company's operations and/or organisational structure, the defined core and sub processes might from time to time be amended.

5. MANAGING OPERATIONAL RISK ASSOCIATED WITH OUTSOURCING ACTIVITIES

When using outsourcing services, the Company ensures that the operational risk inherent in the services used by the Company are also subject to adequate assessment procedures. There should be no distinction between the operational risk management responsibilities of in-house managed activities and outsourced activities.

6. INFORMATION TO MANAGEMENT AND BOARD OF DIRECTORS AND POLICY REVIEW

6.1 Information

When informing the Management and the Board of Directors on operational risk issues, the structures set out in this Policy shall be followed as regards identifying, measuring, categorising, managing and reporting. The operational risks will be reported on a regular basis to the Board of Directors.

6.2 Policy review

The Board of Directors will review this Policy when necessary, depending on the external and/or internal circumstances facing the Company.

OPTIM Investments Limited
30 Saint Georges Street,
3rd Floor, Manor House, Port Louis
www.optimfx.com | info@optimfx.com