



OPERATIONAL RISK MANAGEMENT POLICY

Location Extreme UK Limited

Reviewed & adopted by the Board of Directors on 11 November 20

Contents

1	Purpose	3
2	Definition of operational risk and general approach	3
3	Roles and responsibilities	3
3.1	Role of the Control Committee	3
3.2	Role of the Board of Directors	4
3.3	Role of the President	4
3.4	Role of the Process Owners	4
3.5	Role of the Operational Risk Management Function	4
3.6	Role of the Compliance Office	4
3.7	Role of Internal Audit	5
4	Principles for identifying, assessing, monitoring and controlling / mitigating operational risk	5
4.1	General Principles	5
4.2	Categorisation of operational risk	5
4.3	Structure to identify and manage operational risks	6
4.4	Risk control strategies and guidelines	6
5	Managing operational risk associated with outsourcing activities	7
6	Information to Management and Board of Directors and policy review	7
6.1	Information	7
6.2	Policy review	7

Purpose

The purpose of this Policy document is to define relevant policies and governance to be followed by Location Extreme UK Limited (LX) 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.

This Policy document 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 document 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 ICT, HR and Legal).

1 Definition of operational risk and general approach

Operational risk can broadly be defined as the risk of direct or indirect losses or damaged reputation due to failure attributable to technology, employees, processes, procedures or physical arrangements, including external events and legal risks. In other words, operational risk can be defined as any risk which is not credit risk, market risk, liquidity risk, strategic risk nor compliance risk¹.

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 ICT infrastructure of the Company.

2 Roles and responsibilities

2.1 Role of the Control Committee

The Company has a Control Committee, a supervisory body responsible for the audit of the Company. The main tasks of the Committee are to ensure that the operations of the Company are conducted in accordance with the Statutes and to be responsible for the audit of the Company's annual accounts. In this role, the Committee has an interest to ensure that the operational risk management in the Company is well organised and functions properly.

¹ In other words, the risk of legal or regulatory sanctions, material financial loss or loss to reputation the Company may suffer as a result of failure to comply with laws, regulations, rules, related self-regulatory organisation standards and codes of conduct applicable to its activities.

2.2 Role of the Board of Directors

The Board of Directors is accountable for ensuring that the operational risks at LX are adequately and effectively managed and has the responsibility for establishing a strong operational risk control environment and systems that fulfils the expectations of the member countries of LX, 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.

2.3 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 LX 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.

2.4 Role of the Operational Risk Management Function

The Operational Risk Management Function is responsible for monitoring, coordinating measures, reporting on operational risks and developing the framework models and methodologies as required.

2.5 Role of Internal Audit

Internal Audit is an independent, objective assurance function with reporting lines to the Board of Directors. Internal Audit provides an independent evaluation of the controls, risk management and governance processes. The Internal Audit function shall also independently analyse the work of the Risk Management and Compliance functions.

3 Principles for identifying, assessing, monitoring and controlling / mitigating operational risk

3.1 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 such as the New Product

and Structures Committee or the ICT Council.

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.

3.2 Categorisation of operational risk

The Company has categorised the operational risk event types as follows²:

- | | | |
|----|---|---|
| A. | Internal Fraud | <i>Risk resulting from dishonesty of personnel within the Company, such as forgery of documents, embezzlement, bribery, etc.</i> |
| B. | External Fraud | <i>Risk resulting from dishonesty of individuals outside the Company that causes damage to the Company, such as forgery of financial documents, fraud, etc.</i> |
| C. | Clients,
Products and
Business
Practices | <i>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 unauthorised transactions, unapproved dealings, money laundering activities, or the misuse of confidential customer information, etc.</i> |
| D. | Business
Disruption and
System Failures | <i>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.</i> |
- Point D. includes the following two sub-groups:
- | | | |
|----|---|---|
| 1. | Execution,
Delivery and
Process
Management | <i>Risk 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.</i> |
| 2. | Damage to
Physical Assets | <i>Risk of property damage in the Company resulting from various accidents, such as conflagration, natural disasters, destruction of property, riots, political uprisings, terrorism, etc.</i> |
- | | | |
|----|--|---|
| E. | Employment
Practices and
Workplace
Safety | <i>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.</i> |
|----|--|---|

3.3 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.

3.4 Risk control strategies and guidelines

In addition to this Policy the Company has developed, implemented and maintains an Operational Risk Management Framework, congruent with the Policy. The Framework 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 Framework 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.

4 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. Basically, there should be no distinction between the operational risk management responsibilities of in-house managed activities and outsourced activities.

5 Information to Management and Board of Directors and policy review

5.1 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.

5.2 Policy review

The Policy has originally been approved on 30/10/2017 by the Board of Directors. The Board of Directors will review this Policy when necessary, depending on the external and/or internal circumstances facing the Company.