Fiera Capital Corporation

Operations Risk Management Policy

Approved by the Board on May 9th, 2017

TABLE OF CONTENTS

1. INTRODUCTION

The Enterprise Risk Management ("ERM") framework of Fiera Capital Corporation ("the Corporation", "Fiera" or "FCC") sets out a general structure of roles and responsibilities for the management of key risks across the Corporation: financial, operations, strategic, and legal and compliance risks. The ERM Policy sets out the roles and responsibilities of the Corporation's Board of Directors (the "Board") and the Management Team ("Management") for identifying, evaluating and managing key risks across the enterprise.

Operations Risk Management is an integral component of Fiera's overall approach to Enterprise Risk Management. The Corporation's ability to meet its various stakeholders' requirements on different aspect of its activities depends on its capability to minimize the occurrence and impact of direct or indirect losses resulting from Operations Risk coming from business processes, from IT and infrastructure or from human resources management.

The purpose of this Operations Risk Management ("ORM") Policy is to define the guiding principles and frame boundaries to prudently and proactively manage Operations Risks. The ORM Policy also broadly describes the roles and responsibilities for Operations Risk management within the organization, from the perspective of the Corporation:

- The ORM policy has been developed to comply with, and to supplement, the guiding principles and the framework set out in the the Enterprise Risk Management ("ERM") policy.
- The ORM policy applies the guiding principles and the framework set out in the ERM policy to govern the management of Operations Risks inherent to Fiera' ongoing activities.
- The ORM policy is a formal communication to the entire corporation about Fiera' approach to Operations Risk management.

2. SCOPE & OBJECTIVES

The objective of the ORM Policy is to ensure Operations Risks are managed with reasonable care and with clear roles and responsibilities, and to promote effective management of Operations Risk within management of business processes, IT, infrastructures and human resources across the organization, in order to moderate the likelihood or impact of losses related to Operations Risks.

The ORM Policy is applicable to all operational activities across Fiera and its divisions (the "Fiera Divisions" or the "Divisions") or subsidiaries (the "Fiera Subsidiaries" or the "Subsidiaries").

The ORM Policy focuses on documenting the common definitions, the guiding principles and the governance rules that apply to Operations Risk management across Fiera and its Divisions and Subsidiaries.

More detailed procedures, documented specifically for each of Fiera's Divisions, define the modus operandi for managing different types of Operations Risk at Divisions level.

3. DEFINITIONS

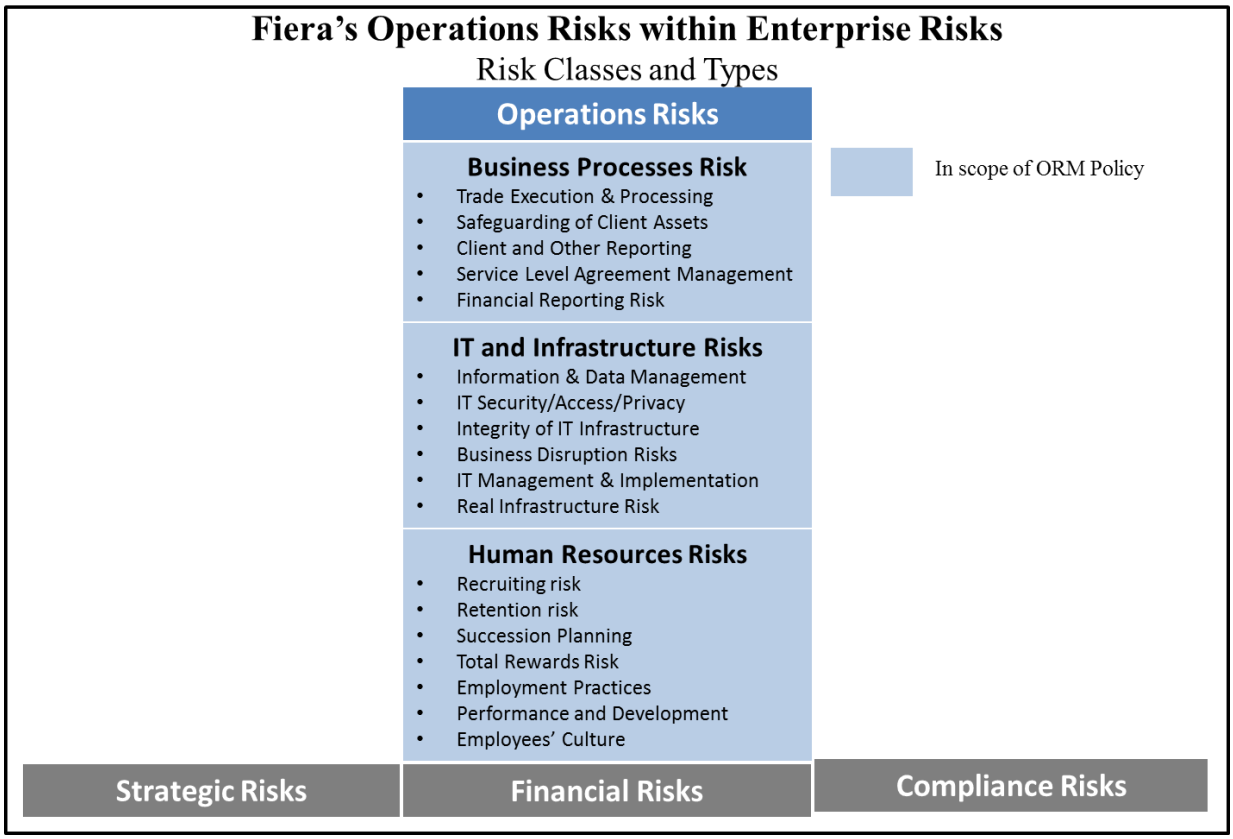
3.1. Operations Risk

Operations Risk is one of the key enterprise risk classes that Fiera Capital is exposed to. As per Fiera's ERM Policy, Operations Risk is defined as the risk of direct or indirect losses resulting from external operational events or from inadequate or failed processes related to business and operations, to IT and infrastructure or to human resources management.

Fiera faces three (3) main types of Operations Risks as illustrated and defined below.

- Business processes risks;
- IT and infrastructure risks; and
- Human resources risks.

Figure 1: Operations Risk Classes and categories of Fiera ORM Policy



3.1.1. Business Processes Risk

1. ***Business Processes Risk:*** It is the risk of a direct or indirect loss resulting from inadequate or failed internal business processes and operations, from ineffective controls, or from external events.

2. ***Trade Execution and Processing:*** It is the risk of failure to execute record and settle trades efficiently and in accordance with and client requirements.

3. ***Safeguarding of Clients Assets:*** It is the risk of failure to adhere to contractual, fiduciary and regulatory obligations with respect to customer assets.

4. ***Client and other Reporting:*** It is the risk of failure to report to clients and other information users in accordance with client requirements.

5. ***Service Level Agreement Management:*** It is the risk of failure to ensure proper service delivery by providers of outsourced services.

6. ***Financial Reporting Risk:*** It is the risk of poor internal controls and inaccurate recording and reporting of financial transactions within existing financial reporting standards, which could lead to misinformed business decisions and could mislead external stakeholders.

3.1.2. IT and Infrastructure Risks

7. ***Information and Data Management:*** It is the risk that data required to produce desired information is unavailable, cannot be obtained in a timely manner, is incorrect or lacks integrity. In includes also the risk of failure to regularly review and monitor defined metrics that are aligned with business needs.

8. ***IT Security, Access and Privacy:*** It is the risk of failure of Information systems to adequately protect the critical data and IT infrastructure from theft, corruption, unauthorized usage, viruses or sabotage.

9. ***Integrity of IT Infrastructure:*** It is the risk of failure to design, manage and maintain adequately the information technology infrastructures to ensure the organization operates in a secure, reliable, well-structured and efficient environment and framework. It includes also the risk of inability to recover from, and continue operations in the event of system failure and/or extraordinary events.

10. ***Business Disruption Risks:*** It is the risk of failure to undertake the appropriate advanced planning related to critical processes to ensure the ability to recover and maintain business operations in the event of a disruption due to physical or natural disasters. It includes threats of business disruption due to natural events and to terrorist activities or other malicious acts.

11. ***IT Management and Implementation:*** It is the risk of failure to prioritize technology initiatives, effectively allocate resources, implement systems and fully support the utilization of these systems in order to achieve the desired major initiatives and the strategic corporate objectives of the Corporation. It includes the risk of IT directly or indirectly contributing to higher operating costs resulting in a material decrease to the company's profitability.

12. ***Real Infrastructure Risk:*** It is the risk of failure to provide physical protection and stewardship over real estate and long-lived assets (such as furniture, equipment, etc.) designed to optimize longevity, value and utilization of those assets.

3.1.3. Human Resources Risks

13. ***Human Resources Risk:*** It is the risk of failure to human resources areas like recruiting, retention, development, engagement and employment practices.

14. ***Recruiting Risk:*** It is the risk of failure to recruit qualified employees to ensure optimal staffing levels in a balanced workforce environment.

15. ***Retention Risk:*** It is the risk of failure to retain qualified employees to ensure a productive and balanced work environment.

16. ***Succession Planning:*** It is the risk of failure to create and implement a succession plan for leadership and key position within the Company.

17. ***Total Rewards Risk:*** It is the risk of not providing competitive financial and non-financial rewards that recruit, develop, retain and recognize our employees within a culture of performance.

18. ***Employment Practices:*** It is the risk of losses arising from acts as an employer that are inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events.

19. ***Performance and Development:*** It is the risk of inability to support the growth and development of employees through effective Performance Management and learning opportunities that are aligned with organizational goals and objectives.

20. ***Employees' Culture:*** It is the risk of inability to promote behaviors and results that are in line with the Company values and goals

4. RELATED DOCUMENTS

- Enterprise Risk Management Policy.
- Investment Risk Management Policy.
- Compliance Risk Management Policy.
- Charter of Fiera's Audit and Risk Management Committee.
- Charter of Fiera's Global Executive Management Team.
- Charters of Divisions' Management Committees.

5. PRINCIPLES, BOUNDARIES AND RULES

5.1. Governance and Oversight

1. ***ERM Policy:*** Principles stated in the ERM Policy govern the management of Operations Risks.

2. ***Division-level roles and responsibilities:*** The Management Committee[1] of each division or subsidiary of the Corporation must define clear roles & responsibilities related to identification, evaluation, management and reporting/monitoring of the different categories of Operations Risks within its division or subsidiary, in line with principles and guidelines documented in the ERM and ORM Policies. For each Division of Fiera, a reporting to the Division's Management Committee must be presented on a regular basis (at least quarterly) to emphasize what are the most important Operations Risks faced by the division and what actions are taken or proposed to manage or mitigate them.

[1] Some Divisions' Management Committees may delegate review of operations risks to a sub-committee.

3. ***Global Executive Management Team reporting:*** The Corporation's Chief Risk Officer ("**CRO**") reports on a regular basis (at least quarterly) to the Global Executive Management Team about Operations Risk management in each Division of Fiera. It is the responsibility of the Divisions' Management Committees to identify which issues and decisions related to Operations Risk in their Division are deemed important enough to be escalated to the Global Executive Management Team and reported by the CRO and the parties involved in these decisions from the Divisions.

4. ***Board reporting:*** The Corporation's CRO reports on a regular basis (at least quarterly) to the Board of Directors (the "**Board**") via the Corporation's Audit & Risk Management Committee (the "**ARMC**") about the Operations Risk management framework.

5. To ensure sound management of Operations Risk, all Fiera's employees should strive to apply the principles below as they engage in managing Operations Risks within their areas:

   - ***Human Resources Risk:***
     a) Recruiting requirements are defined and aligned with Fiera strategy;
     b) Employee performance is regularly appraised;
     c) Succession planning is performed for leadership and key positions, and reviewed yearly;
     d) Procedures related to different human resource events are documented and comply with applicable laws and regulations ; and
     e) Incentive plans are aligned to strategic goals and the achievement of annual scorecards.

   - ***Business Processes Risk:***
     a) Processes are updated and reviewed in accordance with corporate standards and are compliant with all applicable regulatory requirements;
     b) Manual processes are automated where appropriate based on a cost/benefit analysis;
     c) Manual processes, when required, are routinely tracked and subject to reporting on key risks;
     d) All processes are assigned to process stewards responsible for the definition, management, control, integrity and maintenance of the processes;
     e) Operations entrusted to other parties, such as outsourcers or external managers, are subject to a due diligence on a frequency based on the perceived risk of the service provided;
     f) All information used within the organization for the generation of external and/or core control reports (financial statements, clients reports or risk reports) is assigned to an information or data owner: Data owners are responsible for properly defining and maintaining information attributes and access rights for the information;
     g) Information or data owners validate information published within the organization, ensuring that it meets the defined attributes of the information.
     h) All securities and other financial instruments are valued at fair market value in manner consistent with global industry practices as well as applicable laws, regulations and accounting standards;

i) The review and approval of valuation and risk measurement models and controls are performed by a group with the proper training and quantitative skills that is independent of the asset classes.
j) Valuation and risk measurement models are reviewed on a periodic basis.

- ***IT and Infrastructure Risk:***
  a) Systems and data target architectures, as well as development and maintenance methodologies are established and properly controlled to ensure that information technology systems and infrastructure are in line and support Fiera's strategic plan;
  b) Reliance on spreadsheets and end-user tools for data processing, transformation, and storage should be minimal and controlled;
  c) Systems under development are subject to sufficient controls and testing prior to implementation;
  d) Technology development and maintenance is monitored to ensure performance is in line with the organization's needs.
  e) Fiera's assets are subject to adequate physical protection and security: Assets are defined as investments, physical assets (computers, furniture), data and information, and resources.
  f) Technology security processes are tested periodically for accuracy and efficiency to ensure access integrity and security;
  g) All information used within the organization for the generation of external and/or core control reports are protected by effective control measures restricting access to approved personnel;
  h) All transactions performed by Fiera (including investments, purchases, fund transfers, etc.) are required to have sufficient and appropriate managerial review and approval.
  i) External managers overseeing Fiera's assets are subject to a due diligence review upon initial investment and thereafter on an ongoing basis.
  j) Emergency plan and evacuation procedure are documented and regularly exercised to ensure the safety of employees;
  k) Business impact analyses are regularly reviewed and updated to establish clear priorities and maintain a cost-effective contingency strategy;
  l) Business contingency plans are documented and regularly reviewed by individual departments to ensure the continuity of critical processes;
  m) Back-up processes and recovery plans are implemented and tested regularly to ensure the resilience of the information technology
  n) Communication and crisis management plans are documented to promptly and efficiently manage all aspects of a situation beyond the scope of normal operations.

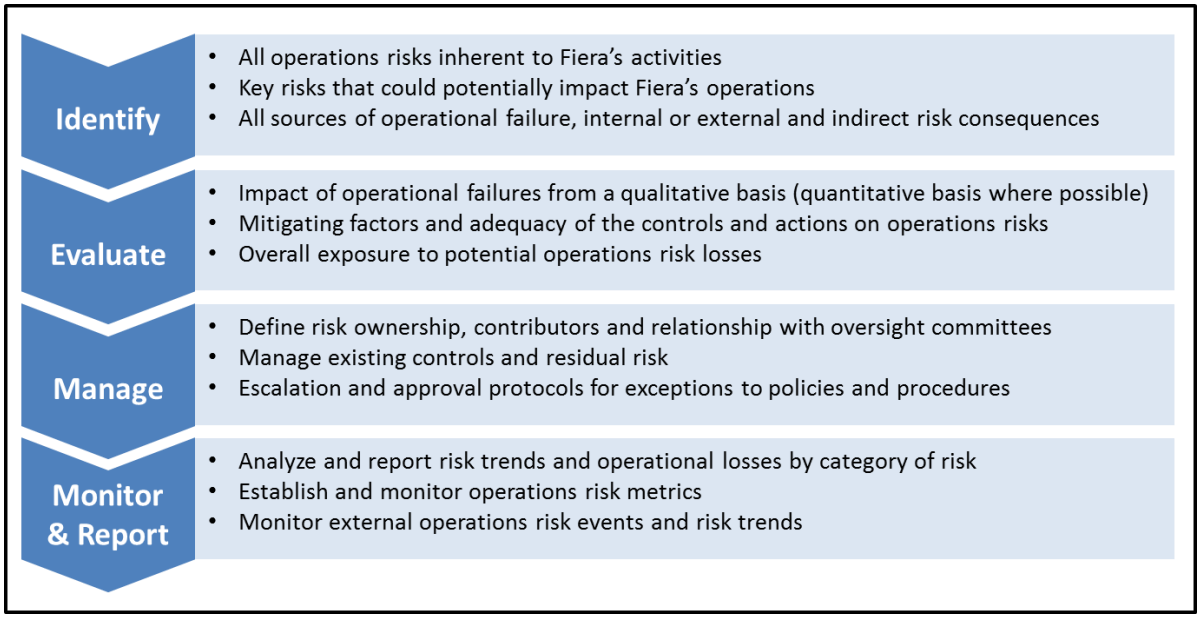
6. DETAILED POLICY SECTIONS

6.1. Framework

1. The ORM Framework (See Figure 2 below) is aligned with the Enterprise Risk Management Framework set out in the ERM Policy. The ORM Framework outlines the broad steps involved in managing Fiera's Operations Risks.

- For each of the Operations Risks identified in the ORM Policy, Fiera's management at each Division is responsible for developing procedures for managing Operations Risk and supplementing the ORM Policy.
- Procedures, tools and other documents, as needed, will also be developed to support the implementation of the respective Operations Risk directives.

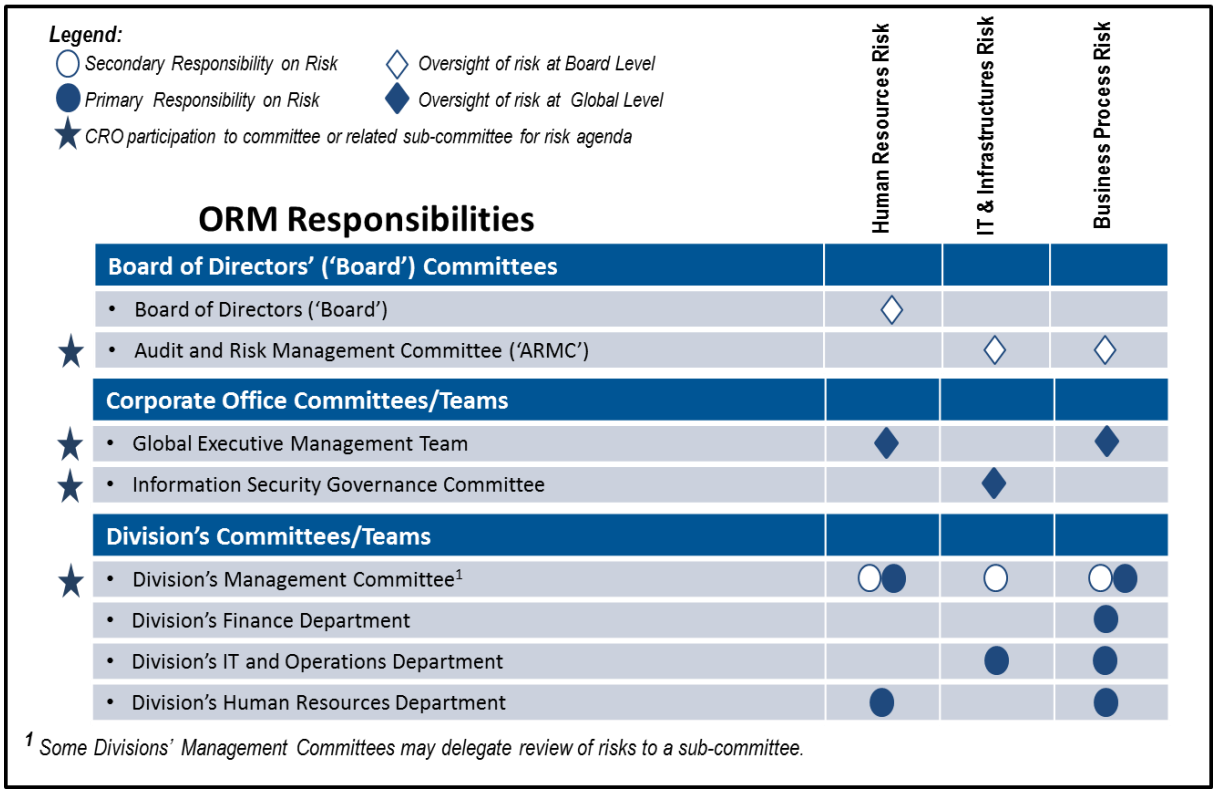
Figure 2: Fiera Capital ORM Framework



6.2. Governance, Responsibilities and Oversight

2. Fiera promotes a risk-aware culture involving all employees.
3. Fiera takes a pragmatic approach to ORM governance that leverages existing committee structures at Corporate and Divisions levels to raise risk awareness and facilitate risk management of Operations Risks.
4. Fiera's ORM Governance structure (See Figure 3 below) outlines the key components of ORM governance within the Corporation's organizational structure where responsibilities of oversight and management of Operations Risks are assigned and fulfilled.
5. The Corporation's Chief Risk Officer (the 'CRO') is mandated by Fiera with the responsibility of overseeing and reporting on operating risks and operating issues across Global and Divisions boundaries that could have a material impact on some of the Global or Divisions' objectives. To do so, the CRO, or one of its representatives, sits on each of the existing committees as described in the ORM Governance diagram in Figure 3, to cover Operations Risk management in the agenda of those committees meetings. It allows the CRO to raise risk awareness and promote and oversee risk management practices at Global and Divisions levels.
6. For each governance layer, core responsibilities for the oversight and management of different Operations Risks are summarized in Figure 3 below.

Figure 3: ORM Responsibilities and Oversight:



7. **Divisions' Management Committee** [2,3]: The Management Committee of each of Fiera's Divisions has responsibility of managing its Division's Operations Risks, by implementing and applying the principles and framework documented in this ORM Policy, and by reporting on key Operations Risks and risk management initiatives to the Global Executive Management Team via its local Division Board of Directors. The Division's Management Committee includes a section of its agenda on Operations Risk management that is coordinated by the Corporation's CRO.

8. **Global Executive Management Team**: The Global Executive Management Team has the ultimate responsibility, among others, of overseeing and approving Fiera's Operations Risk management. It will meet at least on a quarterly basis to have a section of its agenda covering Operations Risk management that will be coordinated by the Corporation's CRO.

9. **Board of Directors (the 'Board')**: the Board has the responsibility to approve the risk oversight and management framework proposed in Fiera's ORM Policy, and to be consulted by the Global Executive Management Team on corporate decisions that could materially impact the Operations Risk profile of Fiera.

10. **Audit and Risk Management Committee (the 'ARMC')**: The Board has delegated to this board-level committee the oversight of the risk management program and practices at corporate level. This committee will meet on a quarterly basis. Any Operations Risk management decision that requires to be escalated at the Board level will be discussed at the ARMC.

[2] For details on the mandate, operating mode and the scope of responsibilities and duties of each existing committee mentioned in this policy, please refer to their charter.
[3] Some Divisions' Management Committees may delegate review of risks to a sub-committee.

7. COMPLIANCE TO POLICY

All employees of Fiera will comply with the ORM Policy. Designated employees will comply with other policies and procedures that relate to specific Operations Risks in the Division they work for.

8. APPROVAL AND REVIEW

The ORM Policy is maintained by the CRO and will be presented to the Board for review not less frequently than every two (2) years.

Document Version Tracking

Version	Date	Modified by	Description
1.0	May 9th, 2017	David Stréliski	Initial Version