GUIDE TO SOUND PRACTICES FOR OPERATIONAL RISK MANAGEMENT

aima
Alternative Investment Management Association

Sponsored by

WELLS FARGO SECURITIES

Table of Contents

GLOSSARY

1. Introduction
1.1 What is "operational risk"?
1.2 Types of operational risk discussed in this Guide

2. Management framework
2.1 Tone at the top
2.2 Governance structure
2.3 Independence of the risk function
2.4 Segregation of functions
2.5 Establishing policies and procedures
2.6 Operational risk reviews
2.7 Regulatory requirements and compliance
2.8 The role of the fund's board of directors

3. Trading, execution and market manipulation risk
3.1 Trading and execution
3.2 Market abuse: market manipulation and insider trading

4. Post-trading risk
4.1 Life of a trade
4.2 Trade processing
4.3 Trade reporting
4.4 Cash movements
4.5 Valuation
4.6 Performance calculations
4.7 Corporate actions and proxy voting

5. Counterparty Risk
5.1 Selection/due diligence
5.2 Credit exposure
5.3 Diversification
5.4 On-boarding and terms
5.5 Key risk measures and monitoring
5.6 Asset safekeeping
5.7 Commission sharing agreements

6. Business conduct and reputational risk
6.1 Codes of ethics and other reputational risk
6.2 Human resources
6.3 Skills and training
6.4 Key persons
6.5 Retention
6.6 Conflicts of interest
6.8 Personal account dealing and personal trading policies

7. Technology and cyber security risk
7.1 Model risk
7.2 Data management
7.3 Systems risk
7.4 Cyber security

8. Business continuity and disaster recovery risk
8.1 BCP plans and testing
8.2 Remote access/alternate sites
8.3 Disaster recovery and support model for key service providers
8.4 Resolution and recovery planning

9. Internal and external fraud and financial crime prevention risk
9.1 Segregation of duties, dual authorisation
9.2 AML/CFT/KYC and financial crime prevention
9.3 Bribery and foreign corrupt practices
9.4 Sanctions

10. Outsourcing risks
10.1 Middle office, back office, IT outsourcing
10.2 Initial due diligence
10.3 Service level agreements
10.4 Ongoing due diligence
10.5 Supervision and monitoring
10.6 Operational monitoring systems

11. Communication risk
11.1 Fund disclosure documents
11.2 Marketing materials
11.3 Performance advertising
11.4 Social media
11.5 Preferential treatment of investors
11.6 Mis-selling

12. Legal, regulatory and compliance risk
12.1 Compliance infrastructure
12.2 Registration and reporting requirements
12.3 Compliance breaches and notifications
12.4 Adherence to contractual terms
12.5 New regulatory requirements
12.6 New markets, investments and lines of business
12.7 Use of external advisors

13. Financial risk
13.1 Financial management
13.2 Regulatory requirements
13.3 Taxation

14.Insurance
14.1 Insurance inventory
14.2 Types of insurance
14.3 Related regulatory/reporting obligations
14.4 Other resources

Appendix A: Top ORM Concerns for New Investment Managers

Appendix B: AIMA Working Group Members

Appendix C: About AIMA

Appendix D: About the Sponsor

Executive summary

AIMA is pleased to present the first edition of its Guide to Sound Practices for Operational Risk Management (the 'Guide'). With the increased scrutiny of hedge fund managers by institutional investors, regulators and the media, particularly post-2008, the focus on a hedge fund manager's operational risk management ('ORM') processes and procedures has multiplied. Following this trend, institutional investors and ORM specialists routinely recommend that emerging managers adopt "sound practices".

There has been other published guidance on the topic of ORM, but AIMA hopes that this Guide will provide additional insights for its manager members looking to improve their operations, and understand what next steps could be considered as an investment manager's AUM grows.

This Guide has been written to be as jurisdiction neutral as possible in order for it to be of the most use to manager members around the world. As a result, there may be specific regulatory requirements which are not discussed in this Guide that will apply to investment managers in various jurisdictions and which may conflict to a greater or lesser extent with what is described in this Guide. Investment managers should comply, first and foremost, with all applicable regulations in their respective jurisdictions.

What is "operational risk"?

Recognising that "operational risk" can mean different things to different people, for purposes of this Guide, we reference the definition posited in 2012 by the Basel Committee on Banking Supervision in its "Principles for the Sound Management of Operational Risk", which states that:

> *"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."*

The Guide uses this definition as a guidepost, however, it does diverge from the Basel Committee's definition by including a discussion of reputational risk which can be a significant risk for investment managers.

Types of operational risk discussed in this Guide

There are many operational risks that an investment manager has to contend with in its day-to-day business, including, but not limited to, business systems risk from internal and external sources, regulatory and outsourcing risk.

Investment managers should strive to implement processes which can help them to effectively identify risks and sources of risk, and put in place procedures to enable control and mitigation of such risks in line with their respective risk appetites.

This Guide focuses on a number of operational risks and includes sections on the following topics:

- **Trading, execution and market manipulation risks** - Trading, execution and market manipulation can be one of the most significant operational risks. This section provides an overview on how the manager should monitor trading and execution. In addition this section describes the oversight needed as it relates to market abuses such as market manipulation and insider trading;
- **Post-trading risks** - Post-trade processing is a critical control function that begins with the verification of trade executions and continues on through reconciliations to trade settlement, regulatory reporting, corporate actions, portfolio performance calculations and valuation calculations. This section provides an overview of the life of a trade (covering issues from segregation of front and back office to monitoring exercises, assignments and expiries), trade processing (covering issues such as trade matching and position reconciliations and breaks management), trade reporting, cash movements (including bank account management and tax), valuation, performance calculations and how to deal with corporate actions and proxy voting (covering issues such as entitlements and key dates);
- **Counterparty risks** - A fund, by virtue of its structure, will have to engage various entities to carry out financial transactions. These relationships subject the fund to counterparty risk. This section focuses on how to select and carry out due diligence on a counterparty, calculating and monitoring credit exposures, the on-boarding process for counterparties and key terms that should be included in agreements, key risk measures and monitoring, asset safekeeping and commission sharing arrangements;
- **Business conduct and reputational risks** - There are a number of key areas that investment managers can focus upon to manage business conduct and reputational risks. This section covers issues such as codes of ethics and other codes of conduct, human resources, skills and training that may be required, the risk of losing a valuable member of the investment manager, retention, transition management, conflicts of interest and personal account dealing and personal trading policies;
- **Technology and cyber security risks** - There are various risks, internal and external, associated with technology and cyber security. This section highlights some of the more common risk areas investment managers should seek to address through a combination of systematic enhancements and employee training. The section covers issues such as model risk, data management and systems risk;
- **Business continuity and disaster recovery risks** - Business continuity is a high priority for investors and regulators hence there is a need to take appropriate steps to mitigate the impact of business interruptions. In order to put an effective plan in place, investment managers should understand the various risks that exist in the disaster recovery process and address these risks with appropriate controls. This section focuses specifically on the risks intrinsic to both internal and external (key service providers) disaster recovery processes and covers issues such as business continuity plans and testing, remote access/alternative sites and resolution and recovery planning;
- **Internal and external fraud and financial crime prevention** - This section describes fraud and financial crime risks and highlights controls and procedures

Executive summary (cont.)

to minimise what could have significant reputational consequences. The section covers issues such as the cash management policy, segregation of duties and dual authorisation, AML/CFT/KYC and financial crime prevention, bribery and foreign corrupt practices and sanctions;

- **Outsourcing risks** - The fund normally outsources investment management activities to the investment manager. The investment manager may then choose to outsource some of these functions to related or third party entities. This section describes risks associated with outsourcing by the investment manager and covers middle office, back office and IT outsourcing. The section includes discussion of the initial due diligence, service level agreements, ongoing due diligence, supervision and monitoring and operational monitoring systems;
- **Communications risks** - To ensure that communications are consistent and represent the views of the investment manager, specific individuals should be given delegations which authorise them to act as spokespeople for the investment manager and to respond to incoming requests from the media and regulators. This section discusses how communications risks can be managed and includes sections on fund disclosure documents, marketing materials, performance advertising, social media, preferential treatment of investors and mis-selling;
- **Legal, regulatory and compliance risks** - While other areas may generate legal, compliance and regulatory issues, there are risks that arise within these functions themselves. This section discusses these risks and covers issues such as the compliance infrastructure, registration and reporting requirements, compliance breaches and notifications, adherence to contractual terms, new regulatory requirements, new markets, investments and lines of business and the use of external advisors;
- **Financial risks** - These are the risks associated not just with the ongoing financial viability of the investment manager, but also with ensuring it meets is financial reporting, audit and taxation obligations. This sections discusses issues such as financial management, regulatory requirements and tax; and
- **Insurance** - The final section of the guide attempts to recognise some of the potential risk-mitigating effects of insurance when applied to an investment manager's operational risks. This section discusses the insurance inventory, types of insurance that may be available and the related regulatory/reporting obligations.

This Guide specifically does not discuss (i) portfolio risks; (ii) liquidity risks; (iii) strategic risks; or (iv) systemic market risks.

To aid emerging managers who are facing operational risk challenges for the first time, we have included in **Appendix A** of this Guide an easy to digest short list of key considerations related to the top organisational risk management challenges.

About AIMA

As the global hedge fund association, the Alternative Investment Management Association (AIMA) has over 1,500 corporate members (with over 9,000 individual contacts) worldwide, based in over 50 countries. Members include hedge fund managers, fund of hedge funds managers, prime brokers, legal and accounting firms, investors, fund administrators and independent fund directors. AIMA's manager members collectively manage more than US$1.5 trillion in assets.

Alternative Investment Management Association

Electronic copies of the full *Guide to Sound Practices for Operational Risk Management (2016)* are available to AIMA member contacts via the AIMA website. The electronic copies are subject to a limited licence and are reserved for the use of AIMA members only.

For further details on AIMA membership, please contact Fiona Treble (ftreble@aima.org), who will be able to assist you.

Disclaimer

The Guide is not a substitute for specific advice, whether legal, regulatory, tax or other advice, nor for professional judgement. It does not seek to provide detailed advice or recommendations on the wider ranging corporate governance issues.