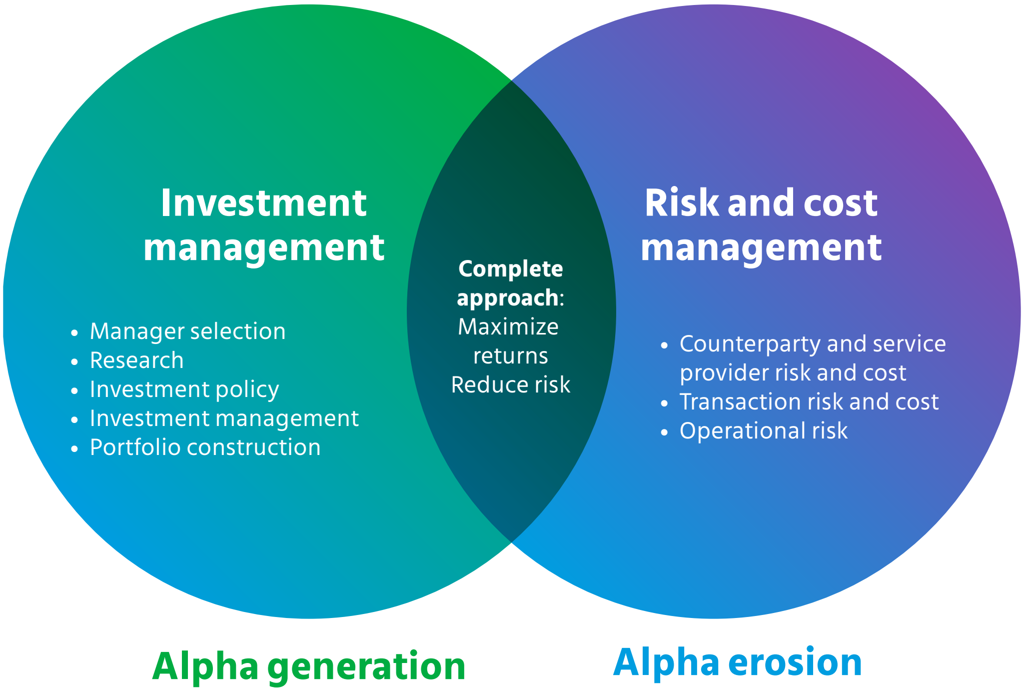
MERCER

The importance of operational due diligence

welcome to brighter

In the oversight of an institutional investment program, the predominant focus is invariably on investment returns and risk management. Asset owners are inundated with information and resources to help manage their investment portfolios. In contrast, operational risks and costs associated with investment implementation and the use of third-party service providers have typically received limited attention. However, prescient investors recognize the increasing complexity of operational processes, regulations and compliance as well as the associated costs and risks.

A comprehensive risk assessment should include a thorough overview of the front, middle and back office functions — that is, investment due diligence (IDD) focusing on "alpha generation" AND operational due diligence (ODD) focusing on the risks and costs of execution that could result in "alpha erosion." The focus of this article is ODD, or the elements of "alpha erosion," which are typically less well understood and less frequently addressed than IDD. It is also worth noting that expert resources in this space are less readily available than in the IDD sector.



Mercer recognizes that nonmarket risks pose unique challenges to investors.

$50B
losses

Madoff Ponzi scheme in 2008

$217M
losses due to an IT coding error

Axa Rosenberg in 2010

$1.6B
losses stemming from an alleged failure to protect segregated client accounts

MF Global in 2011

$6B
losses due to a failure of risk management

JPMorgan Chase in 2012

Mercer defines "operational risk" as the risk of inadequate or failed procedures or policies, systems failures, employee errors, and fraud or other criminal activity.

Mercer defines "operational risk" as the risk of inadequate or failed procedures or policies, systems failures, employee errors, and fraud or other criminal activity. In recent times, several instances of lax due diligence in the operations space have resulted in sizeable losses for companies and their investors. Recent headline-grabbing examples include the case of the Madoff Ponzi scheme in 2008, which resulted in $50 billion losses; Axa Rosenberg in 2010, with $217 million losses due to an IT coding error; MF Global in 2011, with $2 billion losses stemming from an alleged failure to protect segregated client accounts; and Chase in 2012, with $6 billion losses due to a failure of risk management.

What is changing

The historical lack of attention to ODD is changing, particularly in the face of new and evolving regulations that mandate a thorough assessment of operational processes and controls, along with judicious management and oversight of external service providers. For instance, the Australian Prudential Regulation Authority explicitly states that the appointment of an external service provider does not absolve an institution of accountability for such functions, whether investment management or operations management, such as trustee, custodian functions. Similarly, in Singapore, the Guidelines on Outsourcing issued by the Monetary Authority of Singapore (MAS) indicate that any organization outsourcing any of its business activities to an external service provider — particularly material outsourcing arrangements — is required to conduct a self-assessment using these guidelines as a standard. In addition to the internal controls and risk management processes, the MAS also pays close attention to the quality of these institutions' boards and the oversight and governance provided by senior management.

How to get started

An institutional-quality due diligence assessment of operational risks is no different than a comprehensive IDD exercise. It requires specialist resources with an in-depth understanding of industry best practices to evaluate a firm's control environment and asset administration processes within the context of the surrounding investment organization and key service provider relationships. It should comprise detailed assessment of various key subjects, including but not limited to governance and organizational structure, regulation, compliance and audit, transaction execution, valuation and administratio, technology, and third-party relationships.

The primary purpose of an ODD assessment is to benchmark operations and organizational governance against globally accepted safe and sound practices across a broad range of operating procedures, execution practices and internal controls. The outcome of such an exercise is twofold. First, it serves to identify red flags to help an organization avoid substantial financial losses due to operational and organizational deficiencies. Second, it can communicate areas of improvement to the organization to support changes to investment operations that can potentially aid performance and reduce non-investment-related risks.

Sample core topics

- **Governance structure and operating model**
- **Cybersecurity**
- **Cash movement controls and oversight**
- **Valuation**
- **Third-party supervision**
- **Fees and expense ratios**
- **Policies and procedures**
- **Automation**
- **Segregation of duties**
- **Regulatory reporting and adherence**

In the face of a rapidly changing investment and regulatory environment, institutions are being held accountable for managing both investment and non-investment risks. Prudent institutions can no longer afford to be complacent about non-investment-related risks and the potential consequences of ignoring them. Good governance dictates that ODD assessments receive greater focus as institutions seek to meet their fiduciary commitments to their investors. Despite the relative lack of expert resources in this space, institutions are required to be aware of these risks and to actively manage them. The previously prevalent approach of a superficial "check the box" exercise will no longer withstand regulatory scrutiny or satisfy institutions' fiduciary burden to investors. Organizations will now be required to conduct a comprehensive ODD exercise. This exercise should include an assessment of the following factors against global standards and best practices: governance, controls and processes, investment operations and execution risks, and service providers.

Last but not least, ODD should not be viewed as a static exercise; rather, it is a constantly evolving framework of key elements that are critical to the assessment of an organization's middle and back office operations and functions. The risks an organization faces will continue to grow and morph as the market dynamics evolve and the investment and regulatory environments change. A recent case in point is the inclusion of cybersecurity in the ODD assessment in light of the growing recognition that it poses not just a purely technological risk but a key business risk. A farsighted and comprehensive ODD process should therefore continually develop in line with the environment and incorporate new critical aspects of due diligence.

Contact us for more information

Igor Evangelij
Senior Consultant, Mercer Sentinel
+65 6398 2858
igor.evangelij@mercer.com

Petsy Lim
Consultant, Mercer Sentinel
+65 6398 2847
petsy.lim@mercer.com

For further information , please contact your local mercer office or visit our website at www.mercer.com.

6010602-GB

MARSH & McLENNAN COMPANIES