MFDF

MUTUAL FUND DIRECTORS FORUM

The FORUM *for* FUND INDEPENDENT DIRECTORS

Mutual Fund Directors Forum

Role of the Mutual Fund Director in the Oversight of the Risk Management Function

February 2017

Table of Contents

INTRODUCTION

Risk is inherent in the investment management business. At the most fundamental level, investment advisers cannot invest money and earn investment returns without taking some measure of investment risk. Similarly, the systems supporting the operations of a fund are not constructed to eliminate all risks as such a system would defeat the purpose of taking on intended risk. Additionally, these systems cannot totally eliminate "unintended" risk, or all unforeseen and undesirable aspects of expected, or intended risk, as this would be both cost prohibitive, and potentially impossible to execute effectively. Therefore, the goal of effective risk management is not to eliminate risk. Instead, investment advisers and other key service providers develop systems and processes designed to identify risks and manage those risks appropriately in light of the information available.

While boards of directors of mutual funds ("boards" or "fund boards") are not directly responsible for risk management of the funds they oversee, directors should be aware of their fund's adviser's and key service providers' risk frameworks, policies, procedures, and systems in place for identifying, analyzing, and managing risks.

This paper[1] sets forth key concepts and principles relevant to boards.

- The first section of the paper lays out a fund independent director's (also "fund director" or "director") duties and role in risk oversight.
- The second section of the paper sets forth a framework to allow directors to appreciate how investment advisers develop and monitor risk management programs.
- The final section discusses several specific areas of risk facing mutual funds today.

The Forum recognizes that a "one-size-fits-all" approach to risk oversight is not possible given the diversity among funds and fund families and the evolving universe of risks in a dynamic business environment. Consequently, directors should consider the characteristics of the funds they oversee, including fund type, fund size, the assets and number of funds in the fund complex, the structure of management and other service arrangements, fees, vendor management framework, the nature of the investment objectives and the investments used in the funds when consider its role in risk oversight.

Directors should be aware of whether their fund's adviser and key service providers have appropriate risk frameworks, policies, procedures, and systems in place for identifying, analyzing, and managing risks.

DUTIES OF FUND DIRECTORS

Fund boards are charged with overseeing how their funds respond to a complex environment in a rapidly evolving industry. Although boards are not responsible for directly managing the risks their funds face, fund directors do oversee how the fund's adviser manages its risk, including risk oversight of the fund's service providers. Even though risk oversight is inherent in both the investment management business and the director's role, there are no well-defined duties for directors. However, directors can establish a foundation for their legal obligations with respect to risk oversight by developing:

- An understanding of obligations arising under state law, the Investment Company Act of 1940 ("1940 Act") and the Securities Act of 1933 ("1933 Act");
- An appreciation for applicable guidance from courts and the Securities and Exchange Commission ("SEC") and its staff regarding their expectations for directors; and
- An understanding of the most significant regulatory, investment, and operational risks affecting a fund and a familiarity with the risk framework and processes implemented by the adviser to manage and mitigate those risks.

Obligations Under State Law, the 1940 Act, and the 1933 Act

Funds are organized under state laws and, as a result, a director is considered a fiduciary to the fund.[2] As a fiduciary, a director owes two basic duties to the fund, the "duty of care" and the "duty of loyalty."

- The duty of care requires a director to act with reasonable care and skill in light of his or her actual knowledge and any knowledge he or she should have obtained in functioning as a director. Under state law, directors are generally permitted to reasonably rely on experts, including counsel, the fund's adviser, accountants and others.
- The duty of loyalty means that a director owes a duty to protect the best interests of the fund and not to pursue his or her own interests or those of a third party over the interests of the fund. The duty of loyalty also encompasses the duty to act in good faith.

In assessing the actions of directors, courts apply the "business judgment rule." The business judgment rule insulates a director from liability for a business decision made in good faith if: (i) the director is not interested in the subject of the business decision; (ii) is sufficiently informed to make the business decision; and (iii) rationally believes that the business decision is in the best interests of the company.[3]

In addition to state law fiduciary duties, the 1940 Act also imposes duties on directors in three general areas:

- Evaluating fees charged to the fund and valuing the fund's assets
- Dealing with conflicts of interest
- Assessing third-party service providers

Lastly, the 1933 Act also imposes certain legal duties on fund directors with respect to registration statements, requiring a majority of the board to sign the registration statement of a fund prior to its filing and imposing individual liability for any untrue statement of material fact or material omission in the registration statement.[4]

Court and SEC Guidance

The U.S. Supreme Court, the SEC and SEC staff have consistently emphasized that the fundamental obligation of a fund director is to protect the interests of a fund's investors. The SEC[5] and Supreme Court[6] have made clear that requiring a board of directors that is independent of a fund's adviser is a cornerstone of the structure developed in the 1940 Act to protect the interests of fund investors. The SEC staff has historically emphasized that, in order to fulfill their oversight role, fund directors should not be involved in day-to-day management activities of their funds.

As a general matter, effective oversight contemplates that a fund's directors understand a fund's regulatory, investment, and operational risks. To gain an understanding of these risks, directors should:

- Request enough information regarding the fund's activities and the critical services provided to the fund to enable directors to develop an appropriate understanding of the risks inherent in the operation of a fund and to then assess the effectiveness of risk practices and controls implemented by the adviser and other service providers.
- Receive regular updates from the investment adviser regarding the risks associated with outsourced services and how they are being managed.
- Evaluate on an ongoing basis whether fund policies and procedures in place are reasonably designed and effective at preventing the fund's operations from violating applicable federal securities laws.[7]

While fund directors could be tempted to become drawn into the day-to-day operations of a fund and its adviser, such an approach could distract the directors from their primary responsibility: to provide an oversight function and operate as an independent check on those charged with day-to-day management of the fund's activities. These obligations cannot be met, nor can a fund's investment adviser execute its own responsibilities, unless the fund's directors appropriately delegate day-to-day management responsibilities relating to the fund to the fund's investment adviser and other third-party service providers.

Directors, therefore, can concentrate their efforts on overseeing these parties' performance and managing the conflicts of interest that can arise in a fund complex. While a fund director's fiduciary obligations and responsibilities under the 1940 Act and applicable state law remain the same, how these duties should be best executed in a complex, dynamic risk environment will continue to evolve.

Directors can work with outside parties and the fund's investment adviser to oversee how risks are identified and managed. In addition to the adviser's risk management personnel, the chief compliance officer ("CCO") can be an essential tool for boards in overseeing risk management effectively. The CCO plays a role in many aspects of risk management – as part of a fund's compliance controls and procedures the CCO already is involved in oversight of a variety of risk areas, such as those for valuation, securities lending, and disclosure.[8]

THE RISK PROCESS

As part of their risk oversight, fund's directors should discuss with the adviser its risk assessment process and how potential risks are identified and addressed, and how ongoing risks are regularly evaluated, managed, and, or mitigated. The board should appreciate how the adviser identifies the variety of risk concerns appropriate to a particular fund. While there is no standard model or organizational structure for risk management, and investing styles, operations and service providers can vary widely, most risk management programs follow similar principles. Risk management programs are designed to identify, measure, and manage the most significant risks, not to eliminate every risk.

Directors may find it helpful to become familiar with the standard risk frameworks that advisers may use as a foundation for a fund's risk program. There is no single, standard framework used in the industry, although two that are commonly used are COSO and GARP.[9] Regardless of the particular model that is used by the adviser or other service provider, there are significant elements that typically reside in most risk management programs; these elements are discussed in more detail below.

These elements and risk categories can help the adviser and directors by providing a common terminology to discuss the risk management framework. Significant overlap may occur when categorizing a particular risk into a category – for example, some risks, such as valuation, have elements of all three risk categories at right. Similarly, reputation risk can be a by-product of the risk categories listed at right as well as a stand-alone risk.

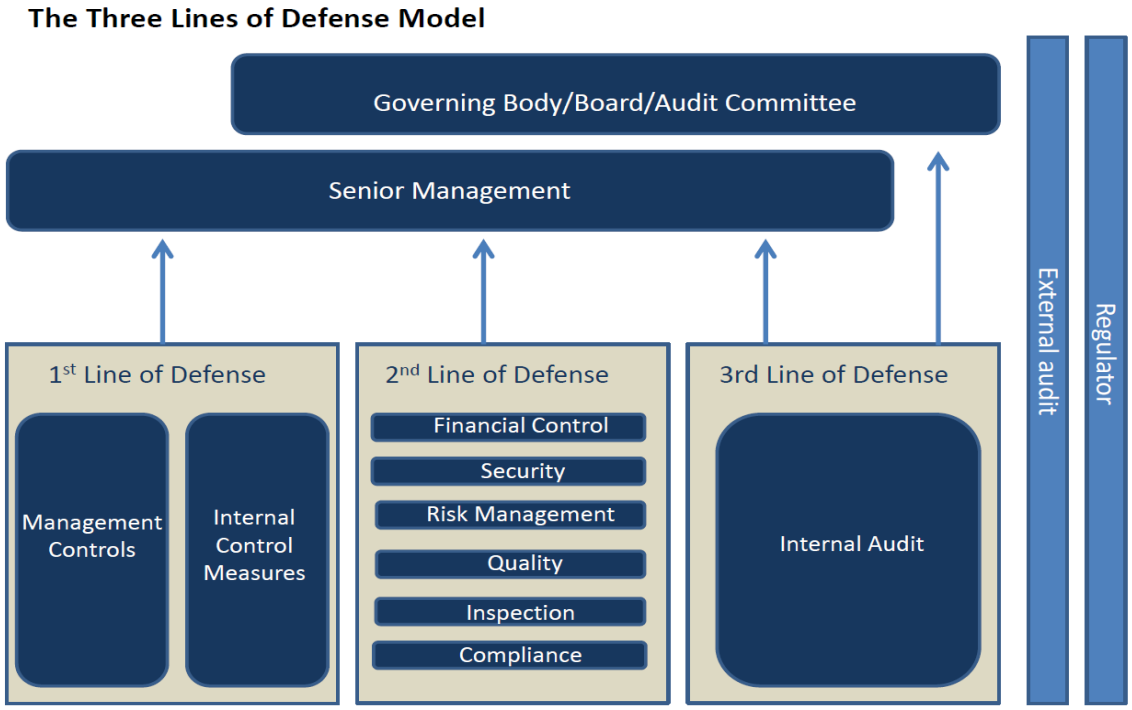
Once risks are identified, an effective risk management program will have a system to organize oversight of those risks. One model that may be used by the adviser is the Three Lines of Defense Model[10] which organizes activities among business functions, risk management, internal audit, management and governing bodies to provide effective risk management. While the three lines of defense do not include the board or any C-Suite executives, both groups play a vital role in the process through oversight and support of the model as well as establishing objectives, strategies, and establishing the structure that governs risk within the organization.[11]

A strong risk management program allows the adviser to identify and manage risks that are relevant to a particular fund and a fund complex.

Risks can evolve over time and will depend on the fund's particular facts and circumstances, such as the fund's investment objective, principal strategies and its operational policies and procedures, outsourced service providers, as well as external forces such as technology and regulatory changes.

In general, risk can be broadly divided into three categories:

- **Regulatory risks**, which are related to regulatory changes and how regulations are interpreted and enforced as well as compliance with various regulations;
- **Investment risks**, which are related to portfolio composition, credit, liquidity, and leverage considerations, among others; and
- **Operational risks**, which include the risks related to people, process, technology, and external events. This is a broad category that includes transaction and control breakdowns, business continuity, system errors or failures, and vulnerability to IT failures and cyber-attacks, among others.



Elements of an Effective Risk Management Program

Tone at the Top and Risk Culture

Tone at the top is a key factor to appreciate when considering the adviser's risk management program. While the tone at the adviser is difficult to empirically evaluate, directors can explore a variety of areas to gain insight into how the adviser views risk. For example, engaging in discussion with senior management, including the fund's chief risk officer (CRO) (provided the fund has a CRO), CCO, chief financial officer, chief investment officer, portfolio manager, general counsel, internal audit, interested trustees, and executives, as well as those outside of the organization such as auditors and outside counsel can help a board understand and appreciate the adviser's attitude toward risk management.

In evaluating the risk culture at a firm, the board also may find it helpful to appreciate how the risk function operates. For example, directors may wish to ask senior management to discuss the roles and responsibilities of the key functions in the three lines of defense framework. In addition, the board also may wish to meet with the specific personnel involved. Boards may find the following questions helpful when considering how the risk function operates within the adviser:

- Which personnel are involved in the risk function, what are their lines of reporting within the adviser's organization, and what are their responsibilities within the risk framework?
- Is the risk management function independent from operating functions within the adviser?
- How is a risk event identified? Once a risk is identified, what is the protocol for response and documentation?
- What kind of risk training is given throughout the organization, including to personnel outside of the direct risk function?
- Who determines which risks are escalated to senior management and the board? What are the criteria for escalating those risks?
- How are risks, risk events and mitigation strategy shared within the organization?

Communication

It is important for a board to understand how the adviser communicates about its risk management program across the organization, including how it notifies appropriate parties about risk events, and how issues are escalated through various levels of management within the organization. The board and the adviser also will want to come to an understanding regarding what information the board receives on a regular basis from the adviser as well as when the board will be notified of risk events. The board should work with the adviser, CCO, risk personnel, fund's CFO and others within the organization to develop a reporting protocol for both the risk management program as a whole as well as for specific risk events, including when information is communicated passed along to the board as well as what information is provided.

As the board considers communication with the adviser regarding risk, the following questions may be helpful:

- How often does the adviser discuss its general risk management program with the board? Who is responsible for these discussions? What should be included in the discussion?
- What kind of reporting does the board receive on a regular basis from the adviser?
- When does the board expect to be notified of a risk event? What is the general process for such communication? What type of information would the board like to receive in such circumstances?
- What are the protocol and severity definitions for communicating with shareholders and intermediaries?
- Has the adviser established relationships with third party public relations experts that can be called upon in case of a risk event?
- What types of risk reporting does the adviser use to manage risk that could also be of assistance to the board?
- Has the adviser established protocols with outsourced service providers for the notification of risk events? Are the protocols part of the agreement with the provider? How are the protocols monitored?

Some questions that a board may wish to ask in order to gauge an adviser's commitment to risk management include:

- Who is responsible for risk management and what is the governance structure?
- Are risk managers within business units or outside of them, or both?
- Has the adviser identified the key risks in each of the key areas – investment, operations, and regulatory?
- What is the process for identifying risk?
- How are the key risks monitored and reported?
- Have there been recent changes to risk practices and/or internal controls?
- What incentives has the adviser put in place to encourage risk conscious behavior?

To assess how executives share risk consciousness throughout the organization boards may wish to ask:

- Do the employees understand the firm's definition of risk and are they familiar with the risk management program's objectives?
- Is there an open dialogue about risk?
- Do employees collaborate on and challenge the development of risk assessments in their areas?
- Are employees encouraged to take personal responsibility for managing risks in their activities (i.e., are all employees risk managers)? If so, how?
- How are risk issues escalated within the organization?
- Are employees hesitant to raise risk issues for fear of retribution?

Risk Appetite and Risk Tolerances

The board may find it helpful to have insight into how the adviser assesses risk in relation to the adviser's risk appetite. Risk appetite defines the amount of risk that the adviser typically tolerates. In defining its risk appetite, different advisers may use different language and concepts. Some advisers classify risk in a qualitative manner (i.e., high, medium, low) whereas others rely on specific quantitative measures.

Another important theme is evaluation of risk tolerance in relation to the overall objectives of a fund. Risk tolerances are statements that set the adviser's expectations for variations around specific objectives. Using risk tolerances can allow management to better monitor whether the fund is operating within its defined risk appetite, which can in turn assist the fund in meeting its objectives.

At an individual fund level, the board can consider whether a fund's strategy is aligned with its risk appetite and risk tolerances. A fund's disclosure documents can help a board determine whether these documents accurately describe the risk of a particular fund. Periodically reviewing a fund's actual risk results against the fund's risk appetite can help determine whether the risk appetite of the fund is in line with the fund's guidelines, position limits, counter-party credit limits, concentration limits, procedures, expected return volatility range, and other similar factors.

While monitoring risk on a fund-by-fund basis is vital, such an approach could inadvertently expose the complex to risk. For example, a risk may be relatively minor for an individual fund, but can have a significant impact on the adviser's organization when aggregated. Therefore, in addition to discussing the fund-by-fund risk, the board also should explore how the adviser monitors risk on a complex-wide basis. Additionally, when the mutual fund complex is only one of the adviser's lines of business, issues in another part of the business may impact the funds. For example, reputational risk arising from another aspect of the adviser's business may impact flows into the fund complex.

Boards may find it helpful to raise the following questions with their funds' adviser:

- What is the adviser's approach to defining risk appetite? If risk appetite principles are not used, how does the adviser monitor risk? Are actual risk results measured against the risk appetite?
- How does the adviser use its risk objectives to inform its activities throughout the organization?
- What does the adviser do when an activity approaches or exceeds the pre-set tolerance level?
- Does the strategy of each fund align with the risk tolerance for that fund?
- Do a fund's disclosure documents accurately communicate its risks? Are risk disclosures consistent between all documents and materials that are in the public domain?
- How does the adviser monitor for aggregate risks across the organization, such as concentration risk?
- Does the adviser compare its risk management processes to best practices?

Risk Process – Identifying, Assessing and Responding to Risks

The adviser's risk management function should include a mechanism to identify risk events such as a cyber breach, a significant trading error, or exceeding the expected volatility range for a fund's return. This step will likely involve personnel from both inside and outside the risk function – emphasizing the importance of internal collaboration and risk training for all employees. The board should discuss with the adviser how it identifies risk events – both established risks and those that may be emerging and the process used to sense and respond to such risks.

Once the adviser identifies a risk event, the next step is the risk response. Although there may not be an immediate response for each risk event (some may be strategic events with longer horizons), it may be helpful for the board to understand how the adviser responds, including the timing, personnel involved, when senior management is notified, and what information is regularly shared with the board.

The following questions may be helpful to directors as they consider how the adviser's risk function operates:

- Does the adviser discuss with the board recent risk events – including how those events were identified, tracked, escalated, reported and addressed?
- Does the adviser learn from issues that arise at other firms and evaluate whether and how it would respond in similar circumstances?
- Does the organization have a risk management playbook that includes escalation and response policies and procedures?
- Has the organization performed simulations of its risk management playbook, and policies and procedures?

Control Activities

Another important element of an adviser's risk management program is control activity which includes management control functions and internal control measures in the business units as part of the first line of defense; oversight functions (i.e., financial controls, risk management, and compliance) in the second line; and assurance provided by internal audit in the third line.

Control activities consist of ongoing development, execution, and evolution of the control structure, and adjustments and responses to address risk events. It may be helpful for a board to understand how each line of defense supports the control structure both with respect to how controls are developed and maintained in the normal course, and when risk events are identified. In addition, boards may wish to ask whether the controls are primarily automated or if they are manual.

In overseeing the adviser's control activities, directors may wish to consider the following:

- How does each line of defense (identified in the three lines of defense model) support the control structure/risk management program?
- How are controls developed and monitored for operating effectiveness?
- How are new risks integrated into the control structure?
- How are risk practices modified based on changes to the internal and external environment in which the fund operates?
- Are the controls operating effectively to manage and/or mitigate the identified risks?
- What controls have been automated?
- Does the adviser monitor automated control activities differently from those that rely on more manual processes? If so, how does the monitoring differ?
- Are there clear lines of responsibility to oversee and manage risks between the legal, risk, compliance, and internal audit functions?
- Does the adviser use third parties to discuss and support risks unique to a particular operation?

Risk Monitoring

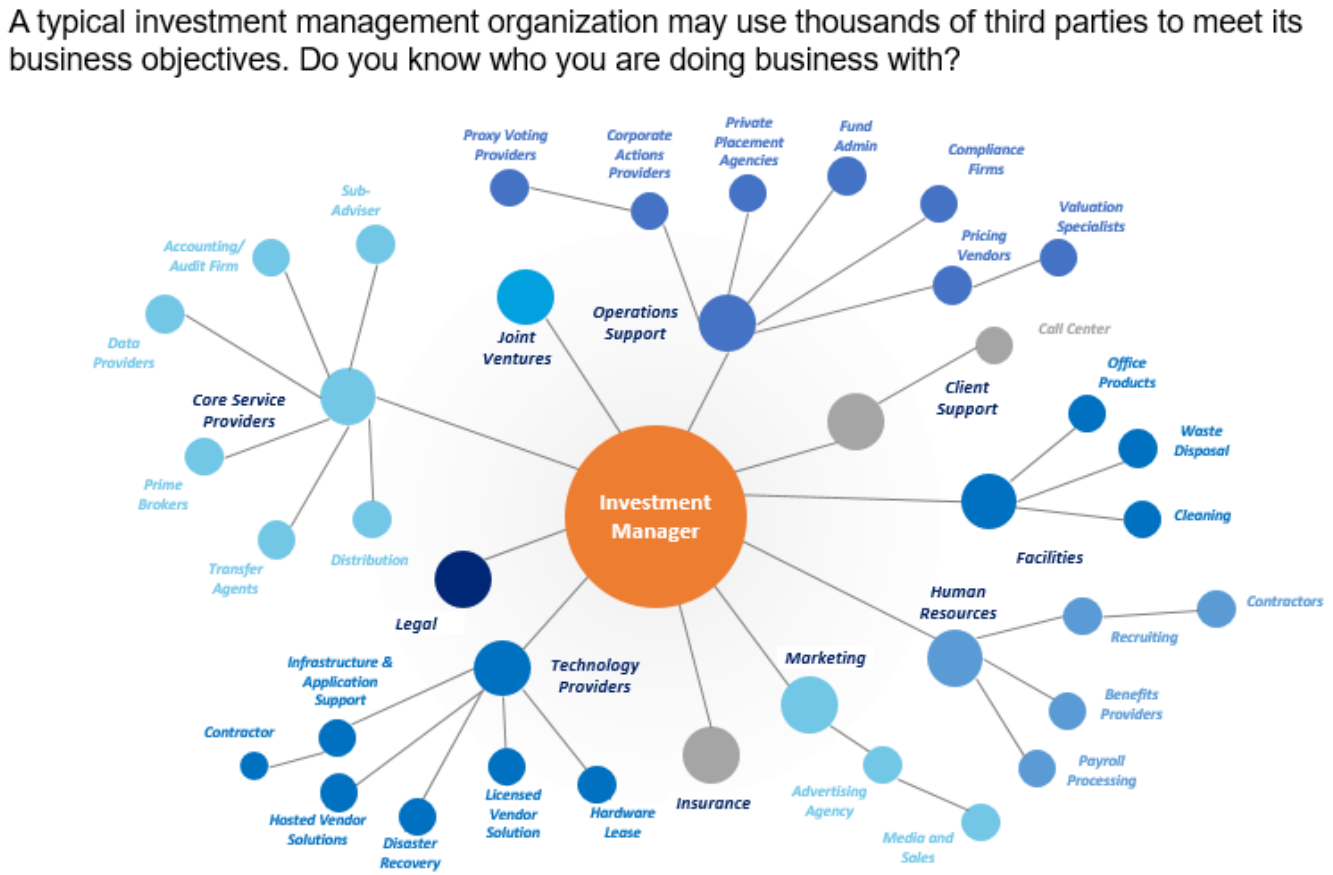
An adviser should continuously evaluate its risk management program in connection with shareholder expectations, current market conditions, and regulatory concerns. In evaluating whether the adviser is appropriately monitoring its risk function, the board may wish to discuss with the CRO (or other appropriate personnel) how the organization monitors the risk management program and determines whether it is functioning as intended. Such a discussion could include how often the CRO (or other risk leaders) conducts reviews of the elements of the fund's risk program; the results of periodic audits or other assessments of the risk management program's effectiveness; and how senior management at the adviser reviews the risk management program to determine whether it continues to meet the fund's needs.

In discussions with the adviser about ongoing risk monitoring, boards may wish to consider the following questions:

- Does the adviser maintain a risk charter or risk inventory that clearly highlights roles and responsibilities and which risks are the focus of the risk management program?
- How does the adviser determine if the risk function is operating as intended?
- Does the adviser conduct periodic audits of the risk function? If so, does it share the results with the board?

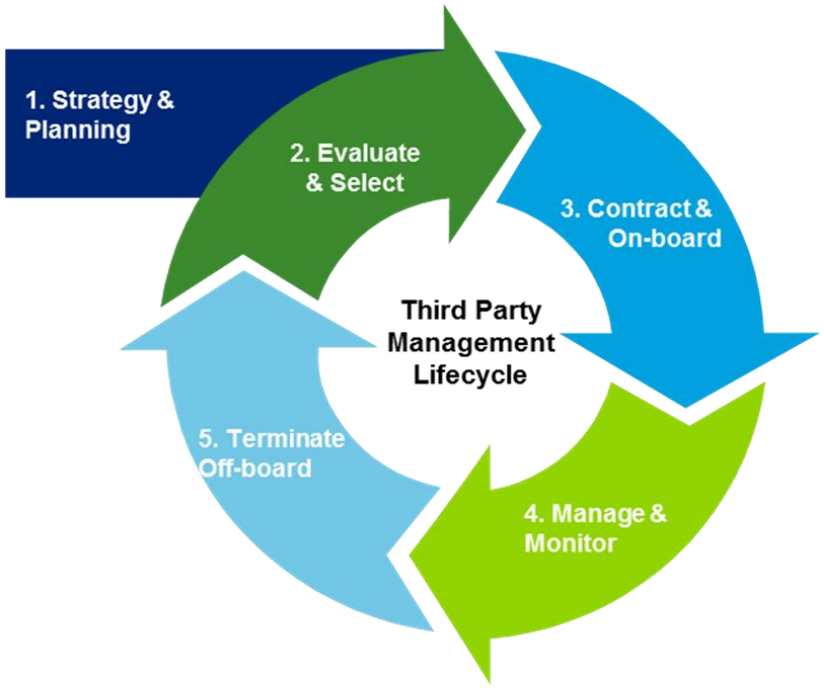
Extended Enterprise Risk Management (EERM)

The mutual fund industry has increased its reliance on third parties to perform a variety of critical functions, including sub-advisers,[12] fund administrators, custodians, transfer agents, other intermediaries, and sub-accounting firms. The chart below illustrates how complex these relationships can be.



Outsourcing a significant portion of non-investment functions exposes the adviser and fund complex to a range of new risks related to the performance of the third party. In addition, the SEC staff's recent guidance and the SEC's rule proposal on business continuity planning will likely result in additional emphasis by the industry on managing the risks associated with outsourced service providers.

The EERM Lifecycle



An EERM program, used to support the risk management program, can assist the adviser in identifying third party risks before they impact the organization. In considering how to manage third parties, the adviser may consider the EERM lifecycle (pictured above) which includes: strategy and planning, evaluating and selecting, contracting and onboarding, managing and monitoring, and terminating and off-boarding). Without a strong third party management program, the fund complex can be exposed to increased risks, including:

- Entering into contracts that incentivize a third party to take risks that are detrimental to the fund or its investors, in order to maximize the third party's revenues
- Failing to effectively weigh risks and direct and indirect costs involved in third party relationships when evaluating service options
- Failing to negotiate an effective service level agreement ("SLA") with the vendor
- Failing to perform adequate due diligence and ongoing monitoring of third party relationships including entering into contracts without assessing the adequacy of a third party's risk management practices
- Engaging in informal third party relationships without contracts or with contracts lacking appropriate risk allocation among the parties.
- Failure to identify critical services to the fund that are not supported by an effective business continuity plan.
- Failure to clearly identify, discuss, and document expectations for the communication of risk events and service level requirements.

Does the adviser have an effective EERM organizational structure with clear roles, accountability, and responsibility - at multiple levels?

While the adviser is responsible for managing risks with a fund's service providers, engaging in a dialogue with the adviser or other service provider may help a board appreciate how the risks of the extended enterprise are being identified and managed. Below are questions that may be relevant to that discussion:

- Who is responsible for the governance and oversight of third parties? Is there a dedicated group (e.g., Risk Committee, Vendor Management, Lines of Business, etc.) for third party risk?
- Do you know where critical services are performed and does vendor management cover these locations from a risk perspective?
- Are the oversight practices (e.g., internal control review, site visits, SLA monitoring, etc.) commensurate with the level of risk the third party presents?
- How is third party risk and the oversight of third parties communicated to the board?
- Does the adviser have the proper "lines of defense" in place? Business Units (first line of defense) are managing third parties day-to-day, Vendor Management/Risk (second line of defense), overseeing and enforcing the enterprise-wide third party oversight program, and Internal Audit/External Auditor (third line of defense) testing the program's effectiveness?
- Does the adviser have mechanisms to manage and track third party performance and contract compliance, including aggregate performance and trends over time?
- Does the adviser have alternative service providers in the event that the adviser would like to make a change?
- Does the adviser have documentation of oversight and escalation activities and relaying information to risk managers?
- Does the adviser have a complete third party inventory? Has the adviser assessed the risks associated with each of the third parties?
- How is the information relayed to the fund's risk managers? The third party's risk managers?
- Does the adviser have an "on-boarding" process to initiate a third party business arrangement?
- Where are the breakpoints, challenges, and potential issues in the fund's third party relationships? How does the adviser assess and stay ahead of them?
- How does the adviser bridge the gap between those in the business and the compliance and risk staff?
- How will evolving technologies, market trends, or disruptive forces present opportunities and challenges to the fund's third party relationships?
- How does the adviser determine whether to outsource or insource, build or buy?
- How does the adviser keep up with the emerging regulatory requirements? Are the fund's third parties keeping up?

Business Continuity Planning

The SEC staff has emphasized the importance of business continuity plans ("BCP") for funds, providing guidance on important considerations in assessing a complex's ability to continue operations following a business disruption.[13] The staff noted the importance of understanding critical service providers' "business continuity planning and disaster recovery protocols" as well as "how the fund complex's own BCP addresses the risk that a critical third-party provider could suffer a significant business disruption."[14]

According to the staff, a fund's critical service providers include those listed in Rule 38a-1 (advisers, principal underwriter, administrator, transfer agent) as well as custodians and pricing agents. The guidance suggests that boards receive annual presentations from the adviser and/or critical service providers, with the participation of the fund's CCO, regarding BCP. In addition, boards may wish to ask the adviser to share the results of tests conducted by the adviser of its business continuity plan.

In discussing an adviser's or other service provider's business continuity plan, boards may find it helpful to ask:

- What were the results of the most recent test of the fund's business continuity plan? How often are the tests conducted?
- How are business outages monitored by the adviser and CCO? When and how are such outages reported to the board?
- How does the fund's business continuity plan address the risk of a disruption at a critical service provider?
- What steps do the adviser and other critical service providers take to mitigate risks associated with business disruptions?

KEY RISKS FACING THE INVESTMENT MANAGEMENT INDUSTRY

The following section will focus on several key risks facing the investment management industry today. However, not all of the risks discussed below will require equal levels of board attention or time during board meetings, nor will they necessarily be addressed by boards in the same way. As directors consider the key risks facing the funds they oversee, they may wish to pay particular attention to areas where there are potential conflicts between the shareholders and the fund's adviser.

Investment Risk

Description of Risk

Oversight of investment risk is a critical component of a director's responsibilities. Investment risk includes both intended or expected risk from the investment process and unintended risk that may result from investment decisions, assumptions, market movements, and other factors. Risk and investment returns are closely linked. Without considering the level and type of risk in a fund's portfolio investments, it is difficult for a director to effectively review the performance of the fund. Every investment alternative contains some form and level of risk and also offers the potential of some measure of theoretical return (positive or negative). Investment professionals generally differentiate between absolute risk and relative risk. Absolute risk generally refers to the variability of the value of an investment whereas relative risk represents the difference in expected return between an investment vehicle or product and an appropriate index or benchmark return. While investment professionals generally agree on how much relative risk is typical for active or passive management products, opinions may differ regarding what level of relative risk is appropriate for a given investment strategy.

In overseeing investment risk, boards may find it helpful to consider the following:

- Evaluating trend levels of investment risk over time
- Comparing returns versus peer groups and benchmark over time on both an absolute and risk-adjusted basis
- Reviewing funds with weak performance more frequently or in a more detailed manner
- Inquiring about unexpected performance results and/or instances of significant over/under performance

Considerations for Fund Directors

- What type and level of investment risks does the manager assume in generating returns?
- Does the manager have systems or resources in place to measure and manage those risks? What are those resources?
- Has the manager demonstrated some core competency in adding value for the level of risk taken?
- How has the value added compared to benchmark and peer groups when measured on a risk-adjusted basis?
- Are the levels (and types) of investment risks in line with a fund's prospectus and SAI?
- Is an appropriate benchmark (of similar risk profile) used for comparison of investment results?
- Are management fees justified by the type and amount of risk taken (i.e., no active fees for a passive product)?
- What types of reporting does the board receive regarding performance attribution? How often do directors receive these reports?
- Is the fund vehicle appropriate for the investment strategy?

Regulatory Risk

Description of the Risk

The current regulatory environment is dynamic and increasingly complex. Each new regulation and interpretive position brings with it the possibility of new requirements that may directly affect the types of risks the board should oversee, as well as how boards carry out their existing oversight responsibilities. In addition to regulations that directly relate to funds, other regulations may have a profound impact on the fund industry as well.[15]

Evolving regulation impacts a fund's internal resources, compliance and internal controls, outsourced services providers, and a fund's systems and technology. For example, a changing regulatory environment may add significant compliance costs which are either absorbed by the adviser or passed onto investors. To avoid these costs, fund advisers may choose to alter their business, types of investments and product lines to avoid or curtail fees that new regulations may bring. In addition to possible compliance costs (or opportunity costs of foregone activities), SEC enforcement activity against a fund can be costly, both in terms of the time and money necessary to defend against a regulatory action as well as possible reputational harm.

Increasingly, directors are being held accountable for breakdowns in a fund's compliance with regulations. Regulators view fund boards as essential in protecting the interests of shareholders.[16] For example, directors have been held accountable by the SEC for breakdowns in both the advisory contract renewal process and in fair valuation.[17] The risk that the board's actions will be reviewed in connection with regulatory matters is ever present.

Increasingly, directors are being held accountable for breakdowns in a fund's compliance with regulations.

Key Considerations for Fund Directors

- What are the latest mutual fund "hot topics"? The CCO, independent legal counsel, independent auditors, industry conferences, and trade organizations can all be valuable sources of information about the latest regulatory developments.
- Do the fund's policies and procedures adequately address the unique risks and challenges posed by each fund in the complex? A "one size fits all" approach can leave funds open to unnecessary regulatory risks by concentrating too heavily on areas that are low risk, looking too broadly at high risk areas of a particular fund, or overlooking potential risk areas altogether.
- How does the CCO monitor the fund's policies and procedures? What reports does the board receive about the CCO's testing?
- How are service providers monitored to determine whether their activities meet regulatory requirements? What type of information does the board receive regarding a service provider's compliance?
- Has the adviser demonstrated its ability to respond to changing regulatory requirements? Has the adviser considered both the impact of individual regulations as well as the cumulative effect of changing regulatory expectations?
- What type of project management and review structure is in place to effectively manage new compliance initiatives? How is the adviser staffed with the skill competencies required to execute on the new regulatory requirements?

Liquidity Risk

Description of the Risk

Recently, few topics have received more regulatory focus than liquidity. The SEC's liquidity rule for funds[18] followed on the heels of a targeted sweep exam on fixed income liquidity which was conducted in response to a distressed debt high yield fund that suspended redemptions. Banking regulations that have impacted market making in fixed income instruments as well as the potential for an increase in interest rates also have contributed to the keen focus on this area.

Relevant Literature

SEC Liquidity Rule Release - http://www.sec.gov/rules/UPDATE.pdf

The SEC's rule 22e-4 defines liquidity risk as "the risk that a fund could not meet requests to redeem shares issued by the fund without significant dilution of remaining investors' interests in the fund." Broadly, liquidity risk includes the risk that:

- The fund does not have sufficient liquid assets to meet shareholder redemption requests in an orderly manner consistent with SEC requirements without harming remaining fund shareholders.
- Established methods to determine liquidity have not been applied consistently and/or accurately.
- Established liquidity determination methods are no longer appropriate, due to changing market conditions or other factors.
- The fund's valuation procedures and policies do not appropriately consider liquidity in the valuation process to achieve accurate security valuations.

The rule places specific responsibilities on fund boards in their oversight of liquidity risk. Fund boards will be required to:

- Approve the fund's liquidity risk management program
- Approve the designation of the administrator for the liquidity risk management program
- Receive a report at least annually regarding the liquidity risk management program, which will include notice of any material changes in the program
- Approve any changes to the fund's highly liquid investment minimum if the fund seeks to change the minimum when already below the established minimum
- Be informed within one day if the fund's illiquid investments exceed 15% of the fund's portfolio.

Another area of focus is the intersection of liquidity and valuation. Illiquid assets frequently have to be fair valued because they often do not have a market price.[19] In addition, fund directors should be aware of the possibility that selling illiquid securities to meet redemptions may result in the fund receiving less than the "fair value" for such securities, risking dilution for the fund's remaining shareholders.

Key Considerations for Fund Directors

Fund directors may wish to consider the following relating to liquidity risk:

- What are the liquidity assessments and classifications in the fund's policies and procedures?
- Who at the adviser is responsible for the execution of the liquidity risk management program? What is the role of the portfolio manager in the process? What is the role of the fund traders?
- How are liquidity determinations challenged? Is back testing performed?
- How does the board monitor compliance with the liquidity risk management program? Has the board considered the effectiveness of controls over the process?
- What information does the board receive regarding the liquidity process and the liquidity risk management program?
- What types of disclosures does the adviser make related to liquidity and/or the liquidity risk management program?
- Does the adviser have a position on the use of swing pricing? Short term? Long term?
- Does the adviser have bank lines of credit in place? Does the adviser have the ability to execute interfund leading? What are the procedures governing the use of interfund lending?
- What types of systems and operating practices are in place to manage the fund's day to day liquidity risk management practices?

Related Resources

- Investment Company Act Section 2(a) (41)
- Rule 2a (41) under Investment Company Act
- Accounting Series Releases 113 and 118
- SEC Money Market Release

Relevant Literature

- ICI Valuation Compendium - http://www.ici.org/pdf/pub_11_valuation_volume1.pdf
- MFDF Report: Practical Guidance for Fund Directors on Valuation Oversight – http://mfdf.org/images/Newsroom/Valuation-web.pdf
- MFDF Report: Risk Principles for Fund Directors - http://www.mfdf.org/images/uploads/newsroom/Risk_Principles_for_Fund Directors_April_2010_Web_Version.pdf

Valuation Risk

Description of the Risk

Valuation risk is the risk that a fund inappropriately determines the value of one or more of its investments, resulting in an inaccurate net asset value for the fund. Under such circumstances, certain shareholders will be treated inequitably, bearing either more or less of returns or losses than he or she would otherwise. Broadly, valuation risk includes the risk that:

- Methods developed by the adviser and reviewed and approved by the board for determining fair value are inappropriate.
- The established methods for determining fair value have not been applied consistently and/or accurately.
- The established methods are no longer appropriate, due to changing market conditions or other factors.

Valuation risk is of particular importance to fund directors because Section 2(a) (41) of the Investment Company Act requires directors to determine the fair value of securities for which market quotations are not readily available. While a board cannot delegate its statutory duty, it may appoint others, such as the fund's investment adviser or a valuation committee, to assist the board in determining fair value and to make the actual calculations pursuant to the fair valuation methodologies previously approved by the directors. According to the SEC, it is incumbent upon fund directors to satisfy themselves that all appropriate factors relevant to the value of such securities have been considered and are consistently followed to determine the method of arriving at the fair value of each security.[20]

Key Considerations for Fund Directors

Directors may find the following questions helpful as they consider a fund's valuation risk:

- What are the valuation methodologies documented in the fund's policies and procedures?
- Who at the adviser is responsible for the execution of the valuation policies and procedures? What is the role of the portfolio manager in the process?
- How are valuations tested?
- How does the board monitor compliance with policies and procedures? Has the board considered the effectiveness of controls over the process?
- What information does the board receive regarding pricing vendors who provide the fund with evaluated prices?
- What kind of periodic testing does the adviser use to test the quality of evaluated prices?
- What are the adviser's policies and procedures regarding pricing overrides? Specifically, how does the adviser identify, evaluate, and approve pricing overrides? Does the board receive reporting regarding overrides?
- Do the valuation policies and procedures identify events where the board must be involved or must be notified?
- Has the adviser identified key valuation indicators for each asset class that notify/involve fund directors of potential price uncertainty in the market?
- Does the adviser consult with pricing experts on difficult and/or complex fair valuation matters?

Cyber Risk

Description of Risk

Companies are beginning to embrace the reality that it is not a matter of *if* but *when* a negative cyber event will impact their organization. Cyber risk is not just ubiquitous, it is pervasive. A mutual fund may invest considerably in locking down its IT systems only to become exposed by a trusted third party (or be the conduit of exposure *to* a third party). Additionally, a fund may have strong internal controls yet fail to include cyber risk as a component of its diligence process when evaluating prospective investments.

According to one study, US companies have an 18.6% chance of experiencing a data breach compromising a minimum of 10,000 records in the next two years.[21] Most asset managers polled, including mutual funds, claim to continually experience attempts against their technology infrastructure. Although the motive is not always clear, the attackers range from teenage hackers to organized criminals to nation-states.

What are the greatest cyber risks to the fund and how are those risks being anticipated, managed and mitigated?

Key Considerations for Fund Directors[22]

- What are the greatest cyber risks to the fund and how are those risks being anticipated, managed and mitigated by the adviser and/or other service providers?
- Is the responsibility and accountability for the creation, implementation, enforcement and updating of an integrated cyber risk management program clearly defined at the executive level?
- Does the overarching cyber risk program include all the domains of a recognized standard (such as the National Institute of Standards and Technology ("NIST")) and is it evaluated by an independent third party on a regular basis?
- Does the management team that addresses cyber risks include senior representatives from executive management, IT, legal, risk management, public relations and compliance/audit?
- Is each component of the cyber risk management program documented, frequently tested and periodically evaluated by independent experts, and what are the results of that testing and audit?
- Are the protocols for reacting to a cyber-risk crisis when it occurs well defined and broadly understood? Are they practiced through simulation exercises? Does the adviser have a plan for communicating with shareholders and other stakeholders, regulators and the media in the event of a cyber breach?
- Are all employees required to participate in regular education and training programs relating to cyber risks?
- What is the total budget and staffing for cyber risk management and how does that compare with peer companies?
- What insurance coverage is available to the fund and its directors and/or the fund's service providers in case of a cyber-risk incident? Is that coverage adequate in scope and amount?
- How does the fund board oversee cyber security related issues? Is cyber risk oversight assigned to a committee? What types and frequency of reports are appropriate? What cyber events are immediately reported to the board? Is there an operational monitoring function (e.g., a Cyber Security Operations Center) in the organization?
- Is the fund board taking steps to self-educate on relevant cyber security issues? Would the board benefit from bringing in an outside cyber security expert for educational purposes? Should board members look into attending other informational sessions or conferences?
- What are the people and process based controls that complement the technology based controls?
- Has counsel reviewed contracts with outside parties to consider appropriate risk allocation for cyber events?
- What are the cyber risk due diligence practices for critical service providers?

Reputational Risk

Description of Risk

Reputational risk can be viewed as a loss of trust in the brand of the fund or an increase in negative perception of the brand that can lead to negative publicity, loss of revenues, asset withdrawals, loss of clients, and loss of key talent. Reputational risk can be either a standalone risk or a byproduct of other risk events. A wide range of events can give rise to reputational risk, including inappropriate or unethical conduct, investments in controversial industries, IT platform failures, and cyber security events. While reputational risk is not a new topic, heightened regulatory scrutiny, increased global interconnectedness, a significantly more digitized world and the rise of social media have increased the speed of onset and potential impact in this area.

Key Considerations for Fund Directors

Directors may wish to consider the following relating to reputational risk:

- Is reputational risk integrated into the fund's enterprise risk management framework?
- How is reputational risk addressed in the fund's risk management governance structure?
- How are risks, events, or activities that can give rise to reputational damage identified?
- How does the adviser stay apprised of the key stakeholders' opinions of the fund complex?
- How does the adviser monitor reputational risk (such as through customer surveys, media monitoring, etc.)?
- Is reputational risk explicitly considered during "new investment, product, or business" evaluation and approval process?
- Is reputational risk explicitly considered during evaluation and monitoring of third party relationships?
- Does the fund have crisis management plans in place that are periodically tested? How are test results reported to the board? What are the escalation points in the fund enterprise to review and respond to reputational brand issues?
- Does the adviser perform "risk sensing" to determine risk considerations related to its brand (*i.e.*, what do people say about the adviser, what are the risk considerations related to competitors' challenges)?
- Has the adviser performed war gaming exercises to reduce the response time and impact to the adviser's reputation in the event of a crisis?

Risk Related to New Strategies

Description of Risk

Advisers often launch new strategies or funds, as well as use new types of complex instruments (including credit default derivatives and emerging markets debt, for example) within existing funds, in an effort to capture growth and yield opportunities in untapped markets, satisfy investor demand and offer customers competitive solutions for their evolving needs. The fund industry has recently witnessed growth in a number of funds, including alternative strategy funds and multi-manager funds with allocations to sub-advisers specializing in alternative strategies. The types and degree of risk and oversight practices will vary depending on the type of fund and the respective policies and strategies to be used by the fund, or the particular risk profile of the new investment vehicle. However, these new strategies or investments can result in heightened leverage, operational risk, liquidity and valuation risk, as well as disclosure risk for the fund complex.

Relevant Literature

MFDF Report: Board Oversight of Alternative Investments - http://mfdf.org/images/Newsroom/Board_Oversight_of_Alternative_Investments_-_January_2014.pdf

Key Considerations for Fund Directors

When approving funds with new strategies or new investments in existing funds, mutual fund directors may wish to consider the following questions:

- What risks do the fund's new strategies and/or new complex investment vehicles pose? Is the new strategy appropriate for an open end mutual fund structure?
- If the fund is sub-advised, is the investment adviser competent on 1940 Act requirements?
- What is the potential impact or risk, if any, on an aggregated basis to the fund adviser?

- If the strategy requires leverage or the new investment introduces leverage into a portfolio, are controls in place to manage and measure leverage?
- Is the adviser able to execute the alternative strategy while also adhering to any limitations on leverage, whether due to regulatory restrictions or policy / strategy restrictions? Are these products periodically stress tested under various historical and hypothetical scenarios?
- What operations and technology support will the new strategy or new investment require? How may existing operations and systems be enhanced to support the new strategy or investment effectively?
- Can existing systems and personnel support these new types of investments?
- Alternative strategies may also introduce new operational functions, such as collateral and counterparty management. If this is the case, how will these functions be supported from a staffing and workflow perspective?
- Are there scale limitations on the adviser's ability to handle a new strategy or investment type?
- If illiquid securities are involved, are effective controls in place for measuring liquidity and meeting regulatory liquidity requirements?
- Are the fund's valuation policies, procedures and controls sufficient to support the investments contemplated by the new strategy or are required?
- Are the new strategies accurately described to investors in the prospectus, fund marketing materials and other fund offering documents? If a fund begins to invest heavily in a new type of investment, has that new investment risk been disclosed to shareholders?
- Are risk disclosures consistent between the fund prospectus, marketing materials and financial reporting?
- If the new strategy involves the use of a sub-adviser (either directly or indirectly in a fund of funds structure), is the sub-adviser experienced in managing the strategy within the confines of a mutual fund regulated under the 1940 Act?
- What changes, if any, need to be made to the fund's control environment?

Model Risk Management

Description of Risk

Mutual funds increasingly rely on many different models for valuation or pricing of financial instruments, risk management, asset selection, allocation of positions between funds, and other operational functions. As the use of models increases, so does model risk. Model risk is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports.

Models can be incorrect or have errors in calculations. Models are also susceptible to IT risks particularly to formula changes, patching and upgrades. Additionally, models may be used inappropriately, for example, when simplifications necessarily embedded in a model are not appropriate for the complex reality of the activity being modeled or when applied to a different environment than intended when designed. The potential impact of using models incorrectly depends on the model, its use, the extent of reliance on the model and the size of the portfolio being modeled.

Key Considerations for Fund Directors

When discussing how the adviser uses models in its operations, directors may find it helpful to consider:

- How does the adviser manage model risk?
- Does the adviser have a model risk management framework? If so, does it contemplate:
    - Model development guidelines that include but are not limited to requirements related to data appropriateness, conceptual soundness, estimation methodologies, and documentation requirements?
    - Implementation and use guidelines, covering responsibilities of model owners and users, including but not limited to proper use of models and ongoing monitoring of model effectiveness?
    - Robust model validation process for new models as well as substantive changes to existing models?
- Does internal audit or a third party perform a periodic audit to determine whether the model is functioning according to its description and plan?
- What type of regular reporting does the board receive on significant model risk, both for specific models and in aggregate?
- How does the adviser ensure consistency with risk disclosures across all fund documents and marketing materials in the public domain?

Disclosure Risk

Description of the Risk

The 1933 Act requires, among other things, a majority of the fund board to sign a fund's registration statement prior to filing, imposing liability for any untrue statements. Thus, fund directors need to be aware of the risk that disclosures and statements could be made in fund documents that are not true.

The SEC has pursued enforcement actions against fund groups for disclosures that have failed to properly inform shareholders of potential risks. In certain cases, these actions were based on a lack of disclosure regarding how a fund's returns would change as the fund grew. In March 2016, SEC staff issued guidance[23] regarding how funds should disclose the potential impact of market conditions, including market volatility. The IM guidance update states *"Clear and accurate disclosure of the risks of investing in funds is important to informed investment decision and, therefore, to investor protection."*[24]

Key Considerations for Fund Directors

Fund directors may wish to consider the following relating to disclosure risk:

- What are the adviser's procedures for updating fund documents and adding new disclosures?
- Does the adviser have a disclosure committee?
- Who at the adviser is responsible for the updating of fund documents and disclosures?
- How are new disclosures reviewed and approved? What is the role of counsel?
- How does the board monitor updates to disclosure?
- Does the adviser perform a periodic update and assessment of all disclosures that includes an analysis of peer fund disclosures?

Anti-Money Laundering (AML) Risk

Description of the Risk

The risk of money laundering and terrorist financing has always challenged the mutual fund industry. However, with increased regulatory pressure on the banking industry and substantial dollars flowing to and from these money laundering and terrorist organizations, funds may be viewed as an alternative place for illicit dollars. Failure for the fund itself to identify potential money laundering scenarios or to comply with regulatory standards can damage the fund's reputation.

Funds are required to have AML and sanctions compliance programs that include:

- Customer identification programs;
- Monitoring and identifying suspicious activity, and timely reporting it;
- Explicit processes for due diligence for foreign correspondent accounts;
- Various reporting and recordkeeping requirements, including requirements to file currency transaction reports and reports in connection with foreign bank and financial accounts;
- Compliance with "special measures" imposed by Financial Crimes Enforcement Network (FinCEN) to address particular AML concerns; training; and
- Independent testing of the AML compliance program.

Key Considerations for Fund Directors

In evaluating a fund's AML policies, directors may wish to ask the following questions:

- Does the adviser have a process to review recent AML enforcement actions to determine whether a fund's AML program, or its policies and procedures should be changed or enhanced?
- Has the fund's administrator, transfer agent or custodial bank been subject to an enforcement action? If so, what, if any, effect did the enforcement action have on the fund's investors?
- Does the fund complex have adequate independent testing to provide an objective assessment about the fund's AML Program?

MUTUAL FUND DIRECTORS FORUM RISK OVERSIGHT WORKING GROUP

Barry Barbash	Partner, Willkie Farr & Gallagher LLP
Joe Berenato	Independent Director, American Funds
Joan Binstock	Partner, Chief Financial Officer - Lord Abbett Mutual Funds, CFO – Lord, Abbett & Co.
James Burns	Partner, Willkie Farr & Gallagher LLP
Joseph Carrier	Chief Risk Officer, Legg Mason, Inc.
Vanessa C. L. Chang	Independent Director, American Funds
Charles Fishkin	The University of Iowa and Bernard M. Baruch College
Paul Kraft	Partner, US Mutual Funds & Investment Advisers Practice Leader, Deloitte & Touche
Brian Liebman	Senior Manager, Deloitte & Touche
Garry Moody	Independent Trustee, AB Funds
Jessica Palmer	Independent Trustee, Goldman Sachs Funds
Charles Rizzo	Chief Financial Officer, John Hancock Group of Funds
Kimberly Saunders	Associate, Willkie Farr & Gallagher LLP
Ralph Verni	Eaton Vance Funds

****

In addition, the following Deloitte professionals provided assistance and content to the overall success of this whitepaper:

- Sean Cunniff, Consulting Specialist Leader
- Maria Gattuso, Advisory Principal
- Joshua Hanna, Advisory Principal
- Olga Kasparova, Advisory Managing Director
- Bryan Morris, Audit Partner
- Mark Nicholson, Advisory Principal
- Tim O'Sullivan, Advisory Managing Director

NOTES

[1] This report has been reviewed by the Forum's Steering Committee and approved by the Forum's Board of Directors, although it does not necessarily represent the views of all members in every respect. The Forum's current membership includes over 887 independent directors, representing 122 fund groups. Each member selects a representative to serve on the Steering Committee. Nothing contained in this report is intended to serve as legal advice. Each fund board should seek the advice of counsel for issues related to its individual circumstances.

[2] Mutual funds are most commonly organized as statutory trusts under Delaware law, corporations under Maryland law, or business trusts under Massachusetts law. Though state law requirements and the organizational documents of a particular mutual fund may vary, the state law concepts discussed in this section are generally applicable to all directors of a mutual fund, regardless of its form of organization.

[3] The business judgment rule, however, does not provide for the exculpation of a director in all cases. In this regard, note that the 1940 Act does not permit a fund to exculpate a board member from liability to which the board member may be subject by reason of bad faith, willful misfeasance, gross negligence or reckless disregard of the board member's duties. *See* Section 17(h) of the 1940 Act.

[4] A mutual fund's investment adviser, and not its directors, typically take the lead in the drafting of a mutual fund's registration statement. In *Janus Capital Group v. First Derivative Traders*, 131 S. Ct. 2296 (2011) ("*Janus*"), the U.S. Supreme Court held that a mutual fund's investment adviser could not be found liable pursuant to an anti-fraud provision of the Securities and Exchange Act of 1934 for misstatements in the fund's registration statement because the adviser did not "make" the statements at issue in the case. The Court ruled that only those who "make" misstatements can be liable, and the Court expressly limited the provision to reach only those who have "ultimate authority over the statement" and those to whom the statement is publicly attributed. While *Janus* did not significantly modify the regulatory framework for registration statement liability, particularly as it relates to fund directors, the case served as a reminder of the importance of a director's role in overseeing a fund's public disclosure.

[5] The SEC indicated, for example, when requiring that a fund's board conduct a self-assessment of its effectiveness, noted that the requirement was designed to strengthen the effectiveness of mutual fund boards as the primary protector of fund shareholders' interests, and that the self-assessment process should focus on strengthening directors' understanding of their role. *Investment Company Governance,* 1940 Act Release No. 26520 at 7 (July 27, 2004) ("Fund Governance Adopting Release") (note: two of the governance provisions adopted in this release were vacated by *U.S. Chamber of Commerce v. SEC*, No. 05-1240, 2006 U.S. App. LEXIS 8403 (D.C. Cir. Apr. 7, 2006). Industry groups have similarly elaborated on this point by advising mutual fund boards to analyze whether board members understand and respect the differences between the board's policymaking and oversight roles and the adviser's operating roles. *See, e.g.,* Report of the Mutual Fund Directors Forum, *Practical Guidance for Mutual Fund Directors: Board Governance and Review of Investment Advisory Agreements* (Oct. 2013), http://www.mfdf.org/images/Newsroom/MFDF_Practical_Guidance_Oct2013_web.pdf. *See also* Independent Directors Council Task Force Report, *Board Self-Assessments: Seeking to Improve Mutual Fund Board Effectiveness* (Feb. 2005), http://www.idc.org/pdf/ppr_idc_self-assessments.pdf. The SEC staff has explicitly stated, "directors play a critical role in policing the potential conflicts of interest between a fund and its investment adviser" and the SEC has concurred, indicating that "[t]o be truly effective, a fund board must be an independent force in fund affairs rather than a passive affiliate of management." *Interpretive Matters Concerning Independent Directors of Investment Companies*, 1940 Act Release No. 24083 at 3 (Oct. 14, 1999); Fund Governance Adopting Release at 3.

[6] *See Burks v. Lasker*, 441 U.S. 471, 482-85 (1979).

[7] *See*, *e.g.*, *J. Kenneth Alderman, CPA, et al.*, 1940 Act Release No. 30557 (June 13, 2013), in which the SEC found former mutual fund directors to have caused their funds to violate Rule 38a-1 under the 1940 Act, which requires a fund registered under the 1940 Act to adopt and implement written policies and procedures reasonably designed to prevent violation of the federal securities laws by the fund.

[8] For more information on the CCO's role, *see The Board/CCO Relationship,* available at http://mfdf.org/images/Newsroom/Board-CCO_Relationship._4.2015.pdf.

[9] COSO is a common framework for enterprise risk management. *See*, the Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework, Executive Summary*, September 2004 (available at http://www.coso.org/documents/coso_erm_executivesummary.pdf) for more details on the COSO framework. The Global Association for Risk Professionals (GARP) also provides a commonly used framework for enterprise risk management.

[10] *See* The Institute of Internal Auditors, *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control,* January 2013 (available at https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf).

[11] *See id.* at 3.

[12] In contrast to third parties that perform a single, critical function, the oversight of sub-advisers may require more attention in light of the breadth of services provided by a sub-adviser. An adviser and board may take longer to get comfortable with a sub-adviser's compliance program if that sub-adviser has not advised a registered fund in the past. For more information on sub-adviser oversight, see the Forum's publications, Practical Guidance for Directors on the Oversight of Sub-Advisers (available at http://mfdf.org/images/Newsroom/Sub-AdviserGuidance.pdf) and Board Oversight of Alternative Investments (available at http://mfdf.org/images/Newsroom/Board_Oversight_of_Alternative_Investments_-_January_2014.pdf).

[13] *See IM Guidance Update No. 2016-04*, June 2016, available at https://www.sec.gov/investment/im-guidance-2016-04.pdf. The SEC also has proposed a rule that would require investment advisers to adopt business continuity and transition plans. *See Adviser Business Continuity and Transition Plans*, SEC Release No. IA-4439, available at https://www.sec.gov/rules/proposed/2016/ia-4439.pdf.

[14] Id.

[15] For example, the Department of Labor's Fiduciary Rule may prove to have a transformative effect on the mutual fund industry. Directors can engage in a dialogue with their fund's adviser about the potential impact of the rule on the particular fund complex as the current compliance date of April 2017 approaches.

[16] Andrew J. Ceresney, Director of the SEC's Enforcement Division recently stated, "as the first line of defense in protecting mutual fund shareholders, board members must be vigilant". *SEC Charges Investment Adviser and Mutual Fund Board Members With Failures in Advisory Contract Approval Process*, SEC Press Release, 6/17/15, http://www.sec.gov/news/pressrelease/2015-124.html

[17] *See SEC Charges Investment Adviser and Mutual Fund Board Members With Failures in Advisory Contract Approval Process,* Press Release, 6/17/15, http://www.sec.gov/news/pressrelease/2015-124.html. *See also In the Matter of J. Kenneth Alderman, CPA; Jack R. Blair; Albert C. Johnson, CPA; James Stillman R. McFadden; Allen B. Morgan Jr.; W. Randall Pittman, CPA; Mary S. Stone, CPA; and Archie W. Willis III,* available at https://www.sec.gov/litigation/admin/2013/ic-30557.pdf.

[18] *See Investment Company Liquidity Risk Management Programs*, 81 FR 82142 (November 18, 2016).

[19] Section 2(a) (41) of the 1940 Act requires directors to determine the fair value of securities for which market quotations are not readily available. See "Valuation Risk for Mutual Funds" below.

[20] See Accounting Series Release 118.

[21] *See 2014 Cost of Data Breach Study: Global Analysis" Ponemon Institute LLC.*

[22] As funds typically outsource operations and other activities to the fund's adviser (and/or other service providers), many of the questions are intended to be directed to the adviser (or other service provider).

[23] *See Fund Disclosure Reflecting Risks Related to Current Market Conditions*, IM Guidance Update No. 2016-02, March 2016 (available at https://www.sec.gov/investment/im-guidance-2016-02.pdf).

[24] Id.