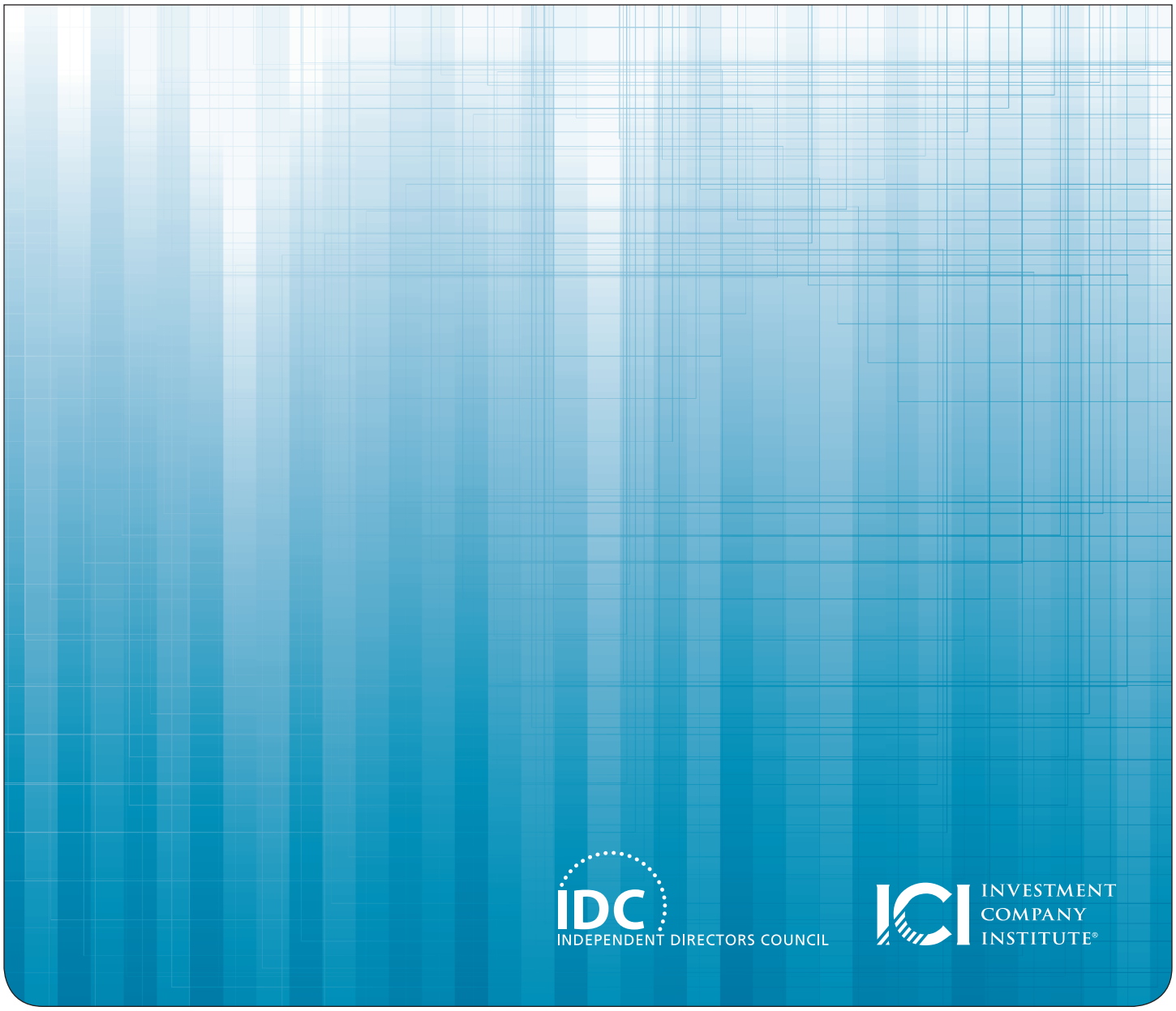
Fund Board Oversight of Risk Management

September 2011



IDC
INDEPENDENT DIRECTORS COUNCIL

ICI
INVESTMENT COMPANY INSTITUTE®

Fund Board Oversight of Risk Management

Contents

Executive Summary

All companies, including registered investment companies (funds), incur risk as a part of doing business. In order to achieve investment returns, a fund must incur investment risks, and the risk of loss arising from daily operations is an unavoidable by-product of any business, including the fund business.

Fund advisers have long been responsible for managing funds' risks. An adviser seeks to optimize investment risk to produce the best risk/reward return for a fund relative to the fund's objectives and risk profile, and the adviser and other service providers manage the operational risks associated with the services they provide to the fund. Fund boards, consistent with their general oversight responsibilities, oversee those activities. The Independent Directors Council (IDC) and the Investment Company Institute (ICI) have written this paper to assist fund directors in understanding and carrying out their risk management oversight responsibilities.

Risk management has attracted increased attention in recent years. Many advisers have recently reevaluated, or are currently reevaluating, their organizational structures and other practices relating to risk management. In many cases, they are adopting more formal risk management practices. Fund boards also have been reevaluating their risk management oversight practices, including the structures and mandates of board committees and the format and frequency of board reports. Practices in the industry continue to evolve.

There are many ways for an adviser to organize the risk management function. Approaches vary depending on a variety of factors, including the adviser's size and resources; the nature of the adviser's (and its affiliates') business; the complexity of the funds' structures and investment strategies; and the size and breadth of the fund complex. It is important to note that an effective risk management program does not necessarily require that an adviser, its parent, or the fund board have dedicated risk management staff, such as a chief risk officer (CRO), or a dedicated risk committee. Regardless of how risk management is organized and implemented, the following recurring themes may serve as a backdrop to a fund board's consideration of risk management processes.

- *"Tone at the top" is critical to promoting a risk-conscious culture.* Senior management's support, reinforcement, and continuing implementation of a robust risk management program are essential for setting a risk-conscious tone in an organization. Fund boards reinforce the tone through their focus and engagement on the topic of risk management.
- *Risk management is a process, not a project.* Risk management is not a one-time or periodic assessment of risks; rather, it should be an ongoing part of business operations. Risk management fills a need not met by individual control functions such as compliance, legal, or internal audit.
- *Risk management is everyone's responsibility.* Each person and business unit in an organization "owns" a piece of risk management.

- *Appropriate independence makes risk management more meaningful.* A process for an independent review of risk controls, assumptions, and models can help to confirm the effectiveness of existing practices and obtain a different and broader perspective of the current risk environment. Independence depends more on respect for the risk management process by senior management and others rather than specific reporting lines for risk management personnel.
- *Risk management is forward-looking and proactive.* To be effective, risk management should seek to identify for management material risks that might impact the fund, the likelihood of them occurring, and the extent of their impact should they occur. Trend reports and other regular, formal processes may facilitate this effort as well as brainstorming sessions and thinking "outside the box." Risk management, however, also can play an important role in analyzing past challenges and recommending changes to prevent their recurrence.
- *Clear communication facilitates effective risk management.* Establishing clear and open lines of communication among interested parties across an organization helps ensure that certain risks do not fall through the cracks and that data and information flowing between business units (including, where relevant, external service providers such as the custodian, fund accountant, and transfer agent) are understood by all to mean the same thing.
- *Organizational structures and policies themselves can serve as risk controls.* Segregation of duties, independence of control functions from business lines, and the use of committees or other, more informal approaches for breaking down "silos" between business units or departments are among a variety of organizational practices that may facilitate effective risk management.

Although the practices of fund boards in overseeing risk management vary and continue to evolve, the board's role and responsibilities generally have been constant.

- *Directors' responsibilities are derived from their general fiduciary duties.* The federal securities laws do not impose any specific obligations on fund directors with respect to oversight of risk management; in general, fund directors' responsibilities are derived from their general fiduciary duties of care and loyalty and are part of their overall responsibility to oversee the management and operation of the fund.
- *A board's focus is on the fund's risks, which also entails understanding the adviser's risks that may impact the fund.* A board's role is to oversee the management of the fund's risks; it is not responsible for overseeing the management of the adviser's risks (or those of its parent or affiliates). Nevertheless, the fund board's focus on the fund's risks will necessarily entail an understanding of the adviser's risks that may impact the fund as well as the associated risk management processes.

» *A board's role is to provide oversight, not to manage risks.* Just as a board does not manage a fund's investments or its business operations, it also does not manage the risks associated with those activities. Board oversight includes understanding the risk management processes employed by the adviser, asking questions where appropriate, and obtaining appropriate assurances that the processes are reasonably designed to manage and control the fund's material risks.

There is no single framework for board oversight of risk management, and a board should fashion its oversight structure in a manner that best suits it and complements its current structure and practices. In addition, just as it does with other governance practices, a board should periodically reevaluate its risk management oversight practices and consider whether any adjustments are warranted. To do so, a board might:

» include risk oversight in its annual evaluation of board effectiveness;

» consider risk oversight as part of any long-term strategy or planning session;

» seek feedback on its risk oversight approach from third parties, such as consultants, external auditors, or fund or board counsel; and

» participate in continuing education opportunities to stay abreast of industry and regulatory developments, including in the area of risk management and oversight, as well as evolving board practices with respect to risk oversight.

Effective risk oversight and management depend on clear communication between the board and the adviser: communication is a two-way street. With the common goal of enhancing shareholder return, fund boards and advisers can support each other in ensuring there is an appropriate focus on optimizing the risks that may benefit fund shareholders and minimizing those that do not.

Introduction and Background

The topic of "risk" and what financial services firms are doing to manage or oversee risk has received heightened attention in recent years. The market events of 2007–2009 prompted many firms to take a fresh look at their practices and resources and to incorporate any lessons learned from their own or others' experience. The Securities and Exchange Commission (SEC) has also focused attention on risk oversight practices by requiring companies, including funds, to disclose the board's risk oversight role.[1] (This paper occasionally uses the term "risk oversight" as a shorthand reference to the board's oversight of risk management.)

Risk management, on the other hand, is not a new concept or function. In the fund industry, a fund's adviser has long been managing a fund's risks as part of its responsibilities for the management and operation of the fund, and the fund's directors have provided oversight of risk management as part of their oversight responsibilities. Practices do vary and continue to evolve.

IDC and ICI have written this paper to assist fund directors in understanding and carrying out their risk management oversight responsibilities. The object of this paper is to bring the rather amorphous subjects of risk and board oversight of risk management to a concrete level, with a focus on funds and the role of fund boards.

This paper primarily addresses the relationship between a fund's board and adviser and their respective roles in addressing risk issues impacting the fund. Some of the discussion may also apply to the fund's relationship with other service providers, such as the fund's administrator, principal underwriter, transfer agent, accountant, and custodian. Those providers also manage the risks associated with the services they provide to the funds. For instance, the transfer agent may manage the risks associated with maintaining shareholder records. This paper does not attempt to address the different service provider relationships a fund may have, but rather, focuses on the adviser, which generally is the fund's primary service provider and may also oversee the services provided to the funds by other service providers.[2]

This paper:

- provides an overview of risk management concepts and fund risks;
- discusses the respective roles of a fund's board and adviser;
- provides insight on risk management and oversight practices in the fund industry, including organizational approaches and risk management tools of the adviser, board committee structures, and risk-related reporting; and
- provides practical guidance for boards.

The appendices provide additional detail and include a list of potential topics and questions for boards to consider in connection with their oversight role (Appendix A); a more focused discussion of investment risk management practices (Appendix B); and a list of common risk terms (Appendix C). Additional resources on risk management are listed at the back of this paper (Additional Resources).

I. Overview of Risk Management

Risk management is an evolving discipline. Several organizations have sought to provide assistance and thought leadership through the development of risk management frameworks and guidance. Much, if not most, of this guidance is focused on traditional operating companies and does not contemplate the externally managed structure of investment companies. As a result, while the guidance these organizations have provided is sound, it typically does not focus on the unique issues faced by funds and their boards of directors. Nevertheless, the concepts and observations in the literature provide helpful insights, and a list of some of these publications is included in Additional Resources.[3]

This section provides an overview of risk management concepts and themes to serve as a foundation for the discussion of practices that follows.

A. Risk Concepts and Definitions

There is no general consensus on how to define various risk-related terms, including the term "risk" itself, and people may have different views on how those terms apply to their particular organization. Both fund boards and advisers would benefit from establishing a common understanding of the terms and concepts they use in risk-related discussions, as well as how they apply to their funds. Some advisers include definitions or descriptions of how they view risk and risk management in their board presentations. They also may explain how they categorize and prioritize types of risks.

A list of common risk terms that might arise in risk-related board reports or board discussions with the adviser is included in Appendix C. Some key terms are listed below.

- *Risk.* A paper titled *Risk Principles for Asset Managers*, written, in part, by a group of buyside risk managers from asset management and fund advisory companies defined risk, "…in a narrow sense, as the possibility of loss or a bad outcome, and in a broader sense, as a neutral measure of the degree to which uncertainty exists about the outcome of an action."
- *Risk management.* The paper defined risk management as, "…the process for identifying, assessing, and controlling both enterprise and portfolio risks in order to minimize unanticipated losses and uncompensated risks and optimize the reward/risk ratio."[4]
- *Enterprise risk management.* Generally speaking, enterprise risk management focuses on the totality of the risks across an enterprise rather than on each of its discrete risks or the risks of individual units or divisions within the organization. It is "a process that provides a robust and holistic top-down view of key risks facing an organization."[5] It also may include a "bottom-up" assessment of risks (i.e., an upward reporting of risk). While the referenced "enterprise" might easily be determined for an operating company, it may not be as apparent in the fund context without some discussion. Accordingly, if this term is used in fund board-adviser discussions, the board may ask the adviser to clarify what constitutes the "enterprise"—e.g., the adviser, its parent organization, the fund complex, or the entirety of the fund's operations, including its service providers.

The definitions in this paper and in Appendix C are intended to serve as a starting point for board-adviser discussions. Boards and advisers may define these terms in a different way from what is presented. Regardless of the definitions used, a common understanding of risk-related terms and concepts, as well as the scope of the adviser's risk management processes, can help to avoid confusion or misunderstanding when discussing risk.

B. Risk Management Themes

There is no single set of "best practices" for risk management in investment companies, but from studies, reports, and other literature relating to risk management generally, as well as the considerable experience of those involved in risk management and risk oversight in the fund industry, some common themes emerge. Regardless of how a fund group's risk management function is organized and implemented, the following recurring themes may serve as a backdrop to the fund board's consideration of risk management processes.

- *"Tone at the top" is critical to promoting a risk-conscious culture.* Senior management's support, reinforcement, and continuing implementation of a robust risk management program are essential for setting a risk-conscious tone in an organization. Fund boards reinforce the tone through their focus and engagement on the topic of risk management.
- *Risk management is a process, not a project.* Risk management is not a one-time or periodic assessment of risks; rather, it should be an ongoing part of business operations. Risk management fills a need not met by individual control functions such as compliance, legal, or internal audit.
- *Risk management is everyone's responsibility.* Each person and business unit in an organization "owns" a piece of risk management. Every employee should be involved in managing the risks within his or her part of the organization. Employees also may seek to be aware of risks that may affect their units but are managed by others, such as information technology risks. Employees and business units have these responsibilities regardless of whether the organization has dedicated risk management personnel, such as a CRO.
- *Appropriate independence makes risk management more meaningful.* A process for an independent review of risk controls, assumptions, and models can help to confirm the effectiveness of existing practices and obtain a different and broader perspective of the current risk environment. Independence depends more on respect for the risk management process by senior management and others rather than specific reporting lines for risk management personnel.
- *Risk management is forward-looking and proactive.* To be effective, risk management should seek to identify for management material risks that might impact the fund, the likelihood of them occurring, and the extent of their impact should they occur. Trend reports and other regular, formal processes may facilitate this effort as well as brainstorming sessions and thinking "outside the box." Risk management, however, also can play an important role in analyzing past challenges and recommending changes to prevent their recurrence.

» *Clear communication facilitates effective risk management.* Establishing clear and open lines of communication among interested parties across an organization helps ensure that certain risks do not fall through the cracks and that data and information flowing between business units (including, where relevant, external service providers such as the custodian, fund accountant, and transfer agent) are understood by all to mean the same thing. Moreover, communication and collaboration among the various control functions (such as risk management, legal, compliance, and internal audit) and business lines foster more informed considerations of risk.

» *Organizational structures and policies themselves can serve as risk controls.* Segregation of duties, independence of control functions from business lines, and the use of committees or other, more informal approaches for breaking down silos between business units or departments are among a variety of organizational practices that may facilitate effective risk management. Although there is a tension between segregating functions and breaking down silos to facilitate information exchange, risk management requires a bit of both.

II. Investment Company Risks

A fund's inventory of risks may be grouped or organized in different ways. One approach is to consider risks within two broad categories—investment risk and business operational risk. A board's focus, though, should be on the key risks to the funds, and not on each discrete risk that exists.

Investment risk is, in absolute terms, the risk of incurring any loss in the portfolio in pursuit of investment return, or, in relative terms, the risk of incurring losses greater than, or of earning gains less than, those of a benchmark index or alternative investment. Sources of investment risks that can affect the performance of the portfolio include market, credit, liquidity, and leverage risk. Appendix B provides a more detailed discussion of investment risk management practices.

Business operational risk refers to the risk of loss that may arise from running a fund business and, in essence, encompasses everything except investment risk. It captures the risks arising from inadequate or failed internal processes, people, and systems, and from external events.[6] The ways in which risks may manifest themselves include: (1) failure in execution, delivery, or process (such as data entry errors); (2) internal fraud (such as insider trading); (3) external fraud (such as forgery); (4) employment practices and workplace safety; (5) problems with clients, products, or business practices (such as failing to protect confidential customer information); (6) business disruption and system failures (such as telecommunications outages); and (7) damage to physical assets (such as from natural disasters).[7] The consequences of risks may be financial, reputational, or regulatory.

In a fund complex, business operational risks may arise within any of the functional units, such as middle- and back-office operations (including shareholder accounting, custody, and fund administration), information technology and security (including securing nonpublic customer data); and human resources (including retention of key personnel). Business operational risk also may include legal and regulatory risks (including compliance risks).

Grouping risks within these two broad categories reflects some important differences. For one, the focus of investment risk management is different than that of managing business operational risks. Because funds are compensated for taking investment risks, the management of those risks entails not only controlling risk exposures, but also optimizing the risk-return of the fund relative to the fund's objectives and risk profile. On the other hand, business operational risks do not typically generate positive returns; thus, the management of these risks entails minimizing them to the extent practicable and subject to reasonable costs. In addition, while investment risks tend to be quantifiable, business operational risks tend to be qualitative and, thus, the risk-related reports for the two categories of risk may be quite different. Some advisers assign responsibility for investment risk management and operational risk management to different people or groups, in part, to draw upon different skill sets (e.g., math or finance for investment risk managers and audit, operations, or compliance for business operational risk managers).

Funds and advisers may use different terms for these categories (e.g., "portfolio risk" for investment risk or "enterprise risk" for business operational risk), or may establish different or additional broad categories of risks, such as compliance/regulatory risk or counterparty risk, around which to organize the risk management function. No matter how an adviser categorizes risks, a board should remember that risks are fluid and do not necessarily fall within mutually exclusive or easily definable categories. For instance, a fund's investment in certain over-the-counter (OTC) derivatives could raise both investment risks (e.g., credit, liquidity, and leverage risks) and business operational risks (e.g., risks associated with processing and tracking the investments). In addition, one risk can lead quickly to other types of risks, such as in the case of default by a counterparty, which could result in an investment becoming illiquid, thereby impacting the fund's compliance with liquidity requirements.[8]

It is also important to note that reputational risk—particularly in the asset management business—is all-encompassing. Reputational risk is not controlled directly; rather, it is an attendant risk that permeates an organization. A material risk event (i.e., an incident leading to an outcome that is different from the expected outcome) in one part of an organization has the potential to adversely affect the reputation of the entire organization. Quantifying reputational risk in any specific case can be extremely difficult given the wide number of relevant variables.

III. Roles of the Fund Board and Adviser

A fund's board and adviser have different roles and responsibilities regarding risk management: the adviser is responsible in the first instance for managing the fund's risks while the board provides oversight of the adviser's activities. Their respective interests in optimizing the risk–return of the fund and in minimizing losses are generally aligned, however. Although the adviser manages its own risks (i.e., its proprietary risks) and is focused on protecting the interests of its own shareholders (or those of its parent), it also manages the risks of its client (the fund) and the two sets of risks are inextricably linked. Successful fund performance can enhance the adviser's brand and reputation, just as a major failure in its services to the fund (or any of its other clients) could have a ripple effect, negatively impacting the adviser's reputation, its relations with its clients, and its overall business.

A. Oversight of Risk Management by Fund Directors

Fund boards are not responsible for managing risks; they provide oversight of others, primarily the adviser, that are responsible for managing risks. Although board practices in overseeing risk management vary and continue to evolve (as discussed in Section V), the board's role and fundamental responsibilities have generally been constant.

1. Directors' responsibilities are derived from their general fiduciary duties. In general, fund directors' responsibilities to oversee risk management are derived from their general fiduciary duties of care and loyalty and are part of their overall responsibility to oversee the management and operation of the fund. Although the SEC requires funds to disclose the board's risk oversight role,[9] the federal securities laws do not impose any specific obligations on fund directors with respect to oversight of risk management. The federal securities laws do, however, impose specific responsibilities on directors, including annual review and approval of the advisory contract, fair valuation of portfolio securities (typically delegated to the adviser), and oversight of the fund's compliance program.[10] By fulfilling these regulatory oversight responsibilities, as well as their fiduciary duties, directors also help to mitigate risks that may impact the fund.

2. A board's focus is on the fund's risks, which also entails understanding the adviser's risks that may impact the fund. A fund board's role is to oversee the management of the fund's risks; the board is not responsible for overseeing the management of the adviser's risks (or those of its parent or affiliates). In fact, the adviser (or its parent) may have its own board of directors or staff overseeing the adviser's risk management processes. Nevertheless, the fund board's focus on the fund's risks will necessarily entail an understanding of the adviser's risks that may impact the fund as well as the associated risk management processes. The fund board's interest is in satisfying itself that the adviser has risk management processes that will serve to appropriately protect the interests of fund shareholders.

The adviser's risks that are relevant to the fund and its board—and the risks that are not—might be the subject of discussion and understanding between boards and advisers. Consider, for example, a situation where the adviser assumes a risk on behalf of another client that does not appear to affect the fund, such as the development of new processes for trading certain derivative instruments that are not consistent with the fund's investment strategy and, thus, in which the fund does not invest. The fund's board may be interested in knowing about these developments and whether they may impact the people, processes, systems, or controls in place for trading the fund's investments.

In board-adviser discussions regarding risk, it may be helpful to clarify whether the referenced risks are those of an individual fund, the fund complex, the adviser, or shared by all. In addition, the board may seek to understand how the adviser's own risks mirror, or differ from, the fund's risks and obtain assurances that the fund's risks are being sufficiently considered and monitored.

3. A board's role is to provide oversight, not to manage risks. Though it is often repeated, it is important to bear in mind that a board's role is one of oversight. A board does not manage a fund's investments or its business operations, nor does it manage the risks associated with those activities. Thus, just as a board's role does not encompass micromanaging the investment decisions of the portfolio manager, it also does not encompass controlling or directly managing the fund's exposures to market, credit, interest rate, or other types of investment risks.

To provide appropriate oversight, fund directors are not expected to be experts in risk management, investment analytics, or a fund's day-to-day operations. Rather, they fulfill their oversight responsibilities, as they do with respect to all fund matters, through the exercise of their business judgment and common sense due diligence. In general, board oversight entails:

- establishing a common understanding with the adviser as to the sources and levels of risk appropriate for the fund;
- being aware of the most significant risks to the fund (including risks of the adviser or its affiliates that may impact the fund) and the steps being taken to manage those risks;
- understanding the current risk management processes, asking questions where appropriate, and obtaining appropriate assurances that the processes are reasonably designed to manage and control the fund's material risks; and
- encouraging and reinforcing a strong "tone at the top" at the adviser by, among other things, sustaining an appropriate focus on risk management.

As discussed in Section V, the board may periodically evaluate its risk oversight processes to ensure their continued effectiveness.

B. Risk Management by Advisers

The fund's adviser and other service providers generally are responsible for day-to-day risk management relating to the fund as part of their responsibilities for the management and operations of the fund; risk management is subsumed within their respective responsibilities. In addition, the adviser's role may include risk management oversight that provides a holistic view of the fund's risks, including those of the adviser and other service providers that might impact the fund.

An additional, important role of the adviser is to assist and support the board in fulfilling its risk oversight role. The adviser may do this by, among other things:

- providing educational sessions on risk management generally or on specific risk topics;
- demonstrating to the board the effectiveness of the adviser's risk management processes to identify, measure, control, and monitor the most significant risks to the fund;
- providing regular, periodic reports on the fund's investment risks;
- identifying and reporting on the fund's most significant business operational risks; and
- escalating material risk-related issues and events to the board when appropriate.

Advisers' practices in managing risks and supporting fund boards vary and are discussed in Section IV.

C. Establishing a Common Understanding Regarding Risk

Communication between the board and the adviser is a critical element of both the adviser's and the board's role in a risk oversight framework. The board and adviser should have a common understanding of the sources and levels of risk that are appropriate for a fund and when a matter should be brought to the attention of the board. For example, the board likely will want to be informed if the adviser intends to invest in a new type of instrument or alter the investment process in a manner that increases the risk profile of the fund. In addition, while a certain level of risk is inherent in all fund operations, the board may wish to be informed if the likelihood of an impact to the fund of a particular risk increases appreciably.

To establish a common understanding in this regard, a fund's board and adviser may want to discuss with respect to specific risks: (1) the potential impact on the fund and its shareholders; (2) the board's and adviser's respective views on the amount of risk that is acceptable; (3) the controls and processes in place and their operating effectiveness; and (4) the resources in place to manage risk (including technology and personnel) and whether additional resources to further mitigate certain risks in a cost-effective manner may be warranted. The board and adviser may have these discussions when a fund is developed and launched; these discussions also may continue as part of the board's ongoing oversight.

IV. Risk Management Practices in the Fund Industry

The risk management function is marked by constant evolution. Advisers continue to evaluate their practices and make adjustments and enhancements to respond to the demands of clients (including funds and their boards), changing circumstances, and new information and technologies. Some have added resources, such as personnel or technology, to support risk management. As the risk management function matures within an organization, it may move from reliance on informal, ad hoc processes to more systematic, formal, and integrated approaches. Nevertheless, there is still a need in risk management for "out of the box" thinking or brainstorming about existing or future risks that does not rely on routine reports.

A. Organizational Structures

There are many ways to structure the risk management function and it is important to note that an effective risk management program does not necessarily require that an adviser, its parent, or the fund board have dedicated risk management staff (including a CRO) or a dedicated risk committee. How the risk management function is fulfilled within the advisory firm, and by whom, may depend on a number of factors including the adviser's size, resources, culture, management structure, and management team as well as the nature of the rest of the adviser's (and its affiliates') business. The complexity of the funds' structures and investment strategies and the size and breadth of the fund complex also are key factors. For example, a fund complex with a limited set of funds and investment strategies may not be exposed to the same level and complexity of risks as would a fund complex with a broader range of funds and strategies. As a result, the adviser to the larger fund complex may have a more expansive risk management infrastructure.

Additionally, the adviser's corporate structure and the regulations governing the adviser's operations (such as international regulations) may influence the adviser's organizational approach. For example, an ICI survey found that advisers whose corporate structures include a bank or insurance company seem more likely to have implemented the position of CRO than those advisers whose business was limited to funds, because federal banking regulators and state insurance regulators have encouraged this structure to better manage and oversee those firms' risks.[11]

Risk Governance Framework

The risk management function may be considered at three levels: risk ownership at the employee and business unit level; risk management across the enterprise; and risk governance by senior management and the adviser's board.[12]

Risk Ownership by Business Units and Employees

Regardless of how risk management is organized within a firm, the people within a business unit are generally responsible for managing the day-to-day risks arising in their units and are likely involved in identifying, measuring, controlling, monitoring, and reporting on these risks. The employees within a business unit—such as the trading desk, information technology, or accounting—generally are in the best position to understand the risks associated with their unit's functions and to develop appropriate controls. Consider, for example, the risk of identity theft. Because a fund's transfer agent is familiar with how accounts are opened and closed and how transactions are processed, employees of the transfer agent generally are in the best position to determine how someone might try to circumvent these processes to commit identity theft. The transfer agent can build controls into its daily processes that are designed to mitigate that risk and monitor the effectiveness of those controls. The transfer agent also may provide reports to the adviser's senior management and the fund board regarding its activities and escalate matters to their attention when appropriate.

In some cases, one or more people within the business unit may be responsible for risk management or may provide risk management support for that unit. For example, the portfolio management group may include risk analysts who generate reports to support the investment management process. In general, the risk analysts do not directly manage a fund's portfolio risks; rather, they analyze and monitor risk exposures and develop reports that can help portfolio managers test the premises and assumptions behind their investment decisions—as well as any models that were developed to implement their investment strategies—and provide insights that the portfolio managers might have missed or discounted. (Appendix B provides more detail about investment risk management and notes that, in some cases, investment risk analysts may reside in a separate group outside of portfolio management.)

Risk Management Across the Enterprise

Each business unit is part of a larger enterprise and has a role in supporting the adviser's (or its parent's or the fund complex's) overall risk management framework by contributing to enterprise-wide risk assessments and escalating risk events or issues. To ensure that all the discrete risks of the various business units are identified, measured, controlled, monitored, and reported, as applicable, an adviser may have a risk management oversight infrastructure that complements, leverages, and oversees the various business units' risk management activities. Such infrastructure would seek to bring commonality to the risk management processes of the multitude of units composing the business, such as through consistent risk assessment methodologies, taxonomies, reporting formats, and escalation procedures. It also would help identify risks that, although acceptable at a unit level, may not be acceptable when viewed at an aggregated level.

This infrastructure may include the following activities.

- Training staff regarding risk management and serving as a consultant on risk management matters;
- Facilitating risk assessments by:
  - developing and overseeing a common methodology and taxonomy for risk assessments;
  - coordinating enterprise-wide risk assessments;
  - aggregating risk assessment results;
  - evaluating results for common themes; and
  - creating a process to support an ongoing risk assessment framework;
- establishing a central place to identify, evaluate, and address new or emerging risks;
- reviewing exposures affecting other industry participants, such as market events or regulatory actions, to consider any applicable lessons to be learned;
- proposing enterprise-wide solutions to common themes arising from risk assessments;
- developing policies and procedures that address, among other things, responsibilities for risk management, escalation procedures, and risk acceptance; and
- providing appropriately calibrated risk reports to senior management, the adviser's (or its parent's) board, and the fund board.

Advisers may employ a wide range of formal and informal means to fulfill this function, and the responsibilities and activities of those who are involved in or facilitate it may vary considerably. The seniority and reporting relationships of those responsible for risk management may also vary across advisory firms.

While informal approaches often play a significant role in the risk management process, the primary formal structures firms use to manage risk are discussed below.

Risk Management Oversight Committee: Some advisers have one or more committees that oversee the firm's risk management program. Risk management oversight committees exist in advisory firms that have dedicated risk management personnel (such as a CRO) as well as in those that do not. When they exist, the composition and mandates of risk committees vary. Some are composed of business unit heads, including those of control groups (e.g., investments, operations, marketing, human resources, legal, compliance, and internal audit). If the firm has a CRO, that person may chair the committee.

The committee structure enables representatives from various parts of the organization to communicate information about, and focus on, risk issues at the enterprise level. Each person can contribute the expertise and knowledge of his or her business unit to facilitate a holistic view of the organization's total risks. Committee mandates vary and may include the responsibility to develop and oversee a common methodology for risk assessments, risk measurements (including of qualitative risks), and policies and procedures to report results to senior management and, as appropriate, to the boards of the adviser and the fund.

Employees with Risk Management Oversight Responsibilities, Such as Chief Compliance Officers: In some cases, typically at the largest firms, one individual is designated as the full-time CRO (discussed below). In other cases, senior management or other staff may be charged with risk management oversight, in addition to serving in their other capacities. Depending on the firm, the CCO may be viewed as a candidate for this role because, among other reasons, he or she already conducts annual compliance-related assessments. Other senior officers, such as the adviser's chief executive officer (CEO), chief operating officer (COO), or chief legal officer (CLO) may be responsible for overseeing risk management within the adviser. In the case of portfolio management risk, the adviser's chief investment officer (CIO) also may be responsible for overseeing risk management.

While such personnel with other responsibilities may be suited to risk management, it is important to note that the risk management role is different from those persons' primary roles. For example, even though a CCO may routinely conduct risk assessments, those assessments generally are limited to compliance risks. The CCO's focus is typically on legal and regulatory risks and may not capture business operational risks—such as retention of key personnel—not typically within the compliance function's purview. Consideration also should be given as to whether the person has the skill set, as well as the time, to take on risk management responsibilities in addition to his or her core responsibilities.

Dedicated Risk Management Personnel, Such as Chief Risk Officers: Unlike the CCO—which funds are required by law to have—there is no legal requirement that a fund or its adviser have a CRO or professional risk managers. Some advisers do, however, have personnel dedicated to the risk management function. Some have a CRO; others may have separate risk officers for investment risk management and business operational risk management. In general, these professional risk officers are not responsible for the day-to-day management of risks.[13] Instead, as noted above, their activities may include training staff and serving as a consultant on risk management matters, facilitating enterprise-wide risk assessments, and providing high-level risk reports to senior management, the adviser's (or its parent's) board, and the fund board.

Reporting structures for risk officers vary: they might report to the CEO, COO, chief administrative officer, CLO, or the chief financial officer, among other possibilities. A reporting relationship to the CEO or executive management team may help to avoid conflicts that might arise if the CRO were to raise issues related to a supervisor's area of responsibility, but other reporting structures can also work well. As noted earlier, senior management's support for the risk management process may matter more than specific reporting lines for risk management personnel.

Risk Governance by Senior Management and the Adviser's Board of Directors

The adviser's CEO and other senior officers are generally responsible for managing risks. They may use a variety of means to fulfill this responsibility, including receiving reports regularly or, when circumstances warrant, special reports relating to risk events or other significant matters. The board of the adviser (or its parent) may oversee the adviser's risk management program, and it also may have a committee with risk oversight responsibilities.[14] An adviser's board is focused on the risks to the adviser's business and potential losses to the adviser's (or parent's) shareholders.

Risk Management's Interface with Other Control Functions

Along with compliance, legal, internal audit, and finance, risk management is a key control function and, thus, is likely to interface on a number of levels with the other control functions. In some cases, the same person may be responsible for two control functions, such as when a CCO also serves as the CRO. Representatives from each of the control functions may participate on a risk management committee or meet with risk management personnel on a regular basis to share information and insights. Internal audit and compliance conduct their own testing and, in some cases, risk management may provide some assistance to them in formulating their audit or work plans. Similarly, risk management may use and rely on testing done by compliance and/or internal audit as part of its activities. Internal audit and compliance also may contribute to any enterprise-wide risk assessment coordinated by risk management, including by providing information about the risks that fall within their particular units. In addition, internal audit may audit the risk management function.

Organizational Structures and Policies That Also Serve as Risk Controls

An adviser may have controls and processes that, though not always expressly designated as "risk management" controls, serve to mitigate risks. For example, some advisers may use committees to bring representatives together from different parts of the organization to focus on a particular subject. A "new investments" committee, for instance, might identify the counterparty, tax, accounting, operational, investment, legal, valuation, and other risks associated with investing in a new type of instrument and determine whether and how those risks could be managed before a fund invests in those instruments.[15] Other committees that may serve to identify and control risks include a credit committee, business continuity committee, and pricing committee. Committees can help to break down silos and promote greater cross-enterprise understanding of issues.

Other organizational structures and policies that may help mitigate risks include:

- segregation of duties;
- independence of control functions from business lines;
- information barriers;
- escalation and exception procedures;[16] and
- compensation structures consistent with the interests of clients, including funds.

Although there is an apparent tension between promoting separation of functions (e.g., segregation of duties and information barriers) and breaking down silos to facilitate information exchange, risk management involves a bit of both. Effective risk management depends on information and, even in those organizations with information barriers and separated functions, it is important that those policies do not impede the flow of data and information necessary to the identification and assessment of risks. Generally speaking, those organizations that take a comprehensive approach to viewing risk exposure from a firm-wide perspective, that share information across the firm, and engage in effective dialogue across the management team tend to be more effective at mitigating risk.[17]

B. Risk Management Tools

Advisers may employ a number of tools and processes to identify, measure, assess, manage, monitor, and document risks. Approaches specific to investment risk management, including common tools and analytics, are discussed in more detail in Appendix B. In general, tools for managing business operational risks may include risk assessments, stress testing and scenario analyses, and a monitoring and escalation process for the most significant risks, as discussed below. Boards may not see all the details of the adviser's use of these tools but may receive reports, at a high level, that summarize the adviser's processes and their results. (See the discussion of board reports in Section V.B.)

Risk Assessments

A risk assessment identifies and analyzes risks within each business unit and across the enterprise. The process may result in an inventory or matrix of risks. Some advisers may rank, rate, or prioritize risks based on the likelihood of occurrence and severity of impact; these risks may be reflected in relative terms, such as "green, yellow, and red" or "low, medium, and high." Unlike many investment-related risks that are quantifiable, many business operational risks are qualitative in nature and, thus, their measurements may be somewhat subjective. For example, the potential loss of key personnel, such as a portfolio manager, may be a qualitative risk not measurable in quantitative terms.

The process also may include an assessment of the controls in place to manage the identified risk so that the risk assessment identifies both the inherent risk and the residual risk that remains after the controls are applied. The residual risk may reflect a significantly mitigated risk as a result of those controls (such as from "red" to "green"). For example, the risk of trading errors may be mitigated by automating key processes. In some cases, the residual risk may exceed a specified tolerance level, and, in those cases, the adviser may develop a remediation plan to enhance controls in order to further mitigate that risk to within acceptable tolerance levels.

The benefits of a risk assessment include identifying risks that had not previously been considered as well as affirming that adequate and effective controls are in place to manage identified risks within tolerance levels.

Stress Tests and Scenario Analyses

Stress tests are required for money market funds, and also are commonly used with respect to other types of funds to evaluate how portfolio investments may perform under certain market conditions or other stresses.[18] Stress tests may also be useful in other areas. For example, business continuity tests often rely upon stress tests or scenario analyses to assess how the fund and adviser would be able to fulfill their business and regulatory obligations in circumstances outside of their control, such as significant and sustained power outages, acts of God, or unforeseen emergencies.

It is important to note that advisers cannot identify all risks that may affect a fund—particularly those arising from "black swan" events—and processes and controls may not eliminate or mitigate the occurrence or effects of all risks.[19] Scenario analyses may help advisers to be better prepared when unexpected events do occur, however. For example, the analyses may help identify information that is difficult to obtain in stressed circumstances so that systems or other improvements may be made in advance of any such situation. Escalation procedures and other advanced planning for incident responses also may help reduce risk exposures when the unexpected does occur.

Monitoring and Escalation

An adviser may monitor and escalate risks through various mechanisms. A risk and control assessment might identify those risks that warrant closer attention or a risk remediation plan, and senior management may receive regular reports regarding the progress of those plans. The adviser also may monitor potential risk trends by using key risk indicators (metrics to provide an early signal of increasing risk exposures in various areas of the enterprise) and/or collecting and analyzing risk events or error or loss reports.[20] Trends, events, or other risk-related matters warranting higher-level attention may be escalated to senior management and, possibly, the boards of the adviser and the fund.

V. Board Practices in Overseeing Risk Management

Fund boards oversee risk management in connection with their various oversight obligations. For example, in discharging their obligations to monitor fund performance and oversee the compliance function, directors regularly assess the quality of the services provided by the adviser and other service providers, including their management of the risks associated with their services to the fund. The advisory contract review process is another context for boards to consider the adviser's risk management practices.

There is no uniform approach to board oversight of risk management and board practices vary and continue to evolve. A board should fashion a risk oversight structure that best suits it and complements its current structure and practices.

A. Board Committees

Many board committees oversee risk as it relates to that committee's mandate. For example, a portfolio performance (or investment) committee may oversee investment risk and an audit committee may consider accounting and financial reporting risks. Indeed, some committee charters specifically include the related risk oversight within the committee's scope of responsibilities.

It does not appear to be a common practice for a board to have a committee whose core mandate is risk oversight. In some cases, though, risk oversight may be assigned to an existing committee, such as the audit committee. In other cases, boards have decided to continue to address risk oversight at the board level, rather than through a committee. They may invite committee delegates to contribute insights from their particular perspectives to the broader discussion.

B. Board Reports

Some risk reporting may be embedded in the regular reports of business units (e.g., compliance risks in the CCO's reports and investment risks in portfolio management's reports). In addition, or alternatively, boards may receive periodic reports on risk management, such as in connection with quarterly meetings or an annual update. Some boards receive investment risk reports quarterly and reports relating to business operational risks less frequently, such as annually. Regardless of the process used to report routine fund business and its associated risks, fund boards may want to ensure that an expedited reporting process exists for reporting material nonroutine or exigent concerns.

Routine Reports

Routine or standard reports a board might receive relating to risk include the following.

Overview of the risk management processes. The adviser could explain the processes it employs to identify, measure, control, and monitor risks affecting the funds and demonstrate their effectiveness. These reports should help the board understand the organizational responsibilities for risk management and the methodologies that are used. The reports might include an educational component about risk management, with definitions of key terms, as well as information necessary to put the report's information in context. The adviser may provide reports on its overall risk management program when changes are made to it or to update the board periodically, such as annually.

Summary reports of fund risks. Boards may receive summary reports of a fund's key risks that focus on pertinent data and information, and the format and content of these reports may be based on the internal reports used by the adviser. Among other things, investment risk reports may provide summary attribution and risk exposure data (see Appendix B for further discussion). The adviser also may provide reports of the fund's most significant business operational risks, such as those that have the greatest potential impact on the fund and its shareholders, as well as the processes in place to control and monitor them or the status of any risk remediation plans. The board may wish to inquire about the methodologies used to determine the particular risks and related information to include in board reports and consider whether they sufficiently capture the board's areas of interest. The adviser may provide more in-depth reporting about new or emerging risks that the adviser or the board has identified as warranting board attention or input. For example, the market events of 2007–2009 may have prompted boards to seek information and analysis regarding the potential risks and impact to the fund arising from the liquidity crisis and the steps being taken to address them. A properly structured risk report should focus on communicating key fund risks to the board rather than significant amounts of facts and statistics.

Stress tests and scenario analyses. Boards also may receive summary reports of any stress tests or scenario analyses that the adviser may have conducted. The reports may explain the methodologies that were followed and provide a summary of the results. If certain scenarios would result in unacceptable losses for some funds, boards and advisers may discuss what actions, if any, may be taken in advance to mitigate those potential losses.

Nonroutine Reports: Escalated Risk Events and Issues

Boards (or committees) also may receive risk-related reports on discrete matters that may materially impact the fund. Similar to approaches with respect to compliance matters, the board may wish to provide guidance to the adviser regarding the matters and circumstances under which it wishes to receive reports about risk events or other issues and how and when such reports should be provided. Some boards may decide to be notified as soon as a significant risk event occurs; others may wish to receive a report once the underlying issue(s) have been addressed and a full report can be provided to the board. Boards also may wish to be notified when the probability of a high-impact event increases significantly, such as when a major hurricane is predicted to reach certain offices. In some cases, the board may designate a director to receive these types of reports between board meetings. While there is no "right" approach to this type of board reporting, both the board and the adviser would benefit from having a common understanding of the process in advance of any such events arising.

C. Educational Sessions

In recent years, many fund boards have scheduled special sessions on risk management to focus on the adviser's risk management program generally, or on discrete topics, such as counterparty risk or business continuity. By focusing on a specific risk area, boards are able to explore in greater depth the potential internal or external events that could trigger a loss or adverse consequence, the controls in place to manage those events or their associated risks, and the effectiveness of those controls.

D. Executive Sessions

Where the adviser has professional risk management staff, such as a CRO, some boards look to and rely on those personnel for risk management information. A board may view the risk officer as charged with observing the adviser's management and operations at a broad level. It should be noted, however, that while regulations require the fund board to approve the designation, compensation, and removal of the fund's CCO, it does not have such regulatory authority over a CRO. Moreover, although the CCO is required by regulation to meet separately with the fund's independent directors at least once a year, there is no such requirement that a risk officer meet separately with the board or its independent directors.[21] Nevertheless, some boards have opted to do so and view the session as an opportunity to engage in a candid discussion about risk matters.

E. Evaluating Board Governance Practices

Consistent with their other governance practices, boards may want to periodically reevaluate their risk oversight practices, such as report formats and frequency, and consider whether any adjustments are warranted. Boards may employ a number of formal mechanisms to evaluate their practices, such as:

- including risk oversight in their annual evaluation of board effectiveness;[22]
- considering risk oversight as part of any long-term strategy or planning session;
- seeking feedback on their risk oversight approach from third parties, such as consultants, external auditors, or fund or board counsel; and
- participating in continuing education opportunities to stay abreast of industry and regulatory developments, including in the area of risk management and oversight, as well as evolving board practices with respect to risk oversight.

F. Disclosure Concerning the Board's Oversight Role

As previously mentioned, funds must disclose in their registration statements the extent of the board's role in the risk oversight of the fund.[23] This disclosure may be prepared by fund management or outside counsel. Fund directors should consider reviewing the draft disclosure or having board counsel review it to confirm that it accurately reflects board practices.

Conclusion

Effective risk oversight and management depend on clear communication between the board and the adviser: communication is a two-way street. Boards and advisers can facilitate effective risk governance by establishing a mutual understanding of risk-related terms and concepts; the sources and levels of risk that are appropriate for the fund; and the content, format, and frequency of risk-related reports to the board. With the common goal of enhancing shareholder return, fund boards and advisers can support each other in ensuring there is an appropriate focus on optimizing the risks that may benefit fund shareholders and minimizing those that do not.

Notes

[1] See Item 17(b)(1) of Form N-1A under the Investment Company Act of 1940 (1940 Act) ("disclose the extent of the board's role in the risk oversight of the Fund, such as how the board administers its oversight function and the effect that this has on the board's leadership structure."); see also Item 18.5.(a) of Form N-2 and Item 20(d)(i) of Form N-3. The risk oversight disclosure requirement became effective February 28, 2010. See Proxy Disclosure Enhancements, SEC Release No. IC-29092 (December 16, 2009). Importantly, this disclosure does not impose any risk oversight responsibilities on fund boards. Instead, it merely requires disclosure of the board's role in such oversight.

[2] See the IDC task force report on *Board Oversight of Certain Service Providers* (June 2007) for more information on the board's role in overseeing these relationships, listed in Additional Resources. In addition, the predecessor to the Financial Industry Regulatory Authority (FINRA) issued a notice discussing considerations relating to oversight of third parties. While the notice applies to fund distributors, and not funds, it may be a useful resource. See NASD Notice to Members 05-48, *Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers* (July 2005).

[3] IDC's previous papers on oversight of derivatives, compliance, certain service providers, and subadvisers are listed in Additional Resources.

[4] Buy Side Risk Managers Forum and Capital Market Risk Advisors, *Risk Principles for Asset Managers* (February 25, 2008) (*Risk Principles*), listed in Additional Resources.

[5] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Effective Enterprise Risk Oversight: The Role of the Board of Directors* (2009). This paper builds upon a previous COSO paper titled *Enterprise Risk Management—Integrated Framework* (September 2004), both listed in Additional Resources.

[6] The Basel Committee on Banking Supervision, a committee of banking supervisory authorities from several countries, defines operational risk this way for purposes of bank regulation. Its definition also specifically includes legal risk but excludes strategic and reputational risk. See Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework* (June 2006) (Basel II). Advisers may determine to define business operational risk differently.

[7] These are types and examples of operational loss events included in U.S. banking regulators' risk-based capital adequacy framework related to implementation of the Basel II standards (see id.). Although the regulations do not apply to funds, they contain this useful framework for thinking about operational risk. See *Risk-Based Capital Standards: Advanced Capital Adequacy Framework—Basel II,* 72 Fed. Reg. 69288 at 69314 (December 7, 2007).

[8] For additional information about board oversight of derivatives, including derivatives-related risks, see IDC's task force report, *Board Oversight of Derivatives*, listed in Additional Resources.

[9] See n. 1, supra.

[10] See Sections 2(a)(41) and 15(c) of the 1940 Act and Rule 38a-1 under the 1940 Act. For additional information about board oversight of valuation, see ICI/IDC's publications, *Fair Valuation Series: An Introduction to Fair Valuation* and *Fair Valuation Series: The Role of the Board*. For additional information about board oversight of compliance, see IDC's task force report, *Board Oversight of Fund Compliance*, listed in Additional Resources.

[11] See Investment Company Institute, *Chief Risk Officers in the Mutual Fund Industry: Who Are They and What is Their Role Within the Organization?* (2007) (CRO Survey), listed in Additional Resources. The survey noted that while there appears to be no regulatory requirement that a banking institution or insurance company have a CRO, many institutions have responded to regulators' interest in having highly experienced senior managers oversee the institution's internal controls by establishing the position of CRO.

[12] See generally Deloitte & Touche LLP, *Risk Intelligent Enterprise Management: Running the Risk Intelligent Enterprise™*, listed in Additional Resources.

[13] See CRO Survey, supra n. 11.

[14] The New York Stock Exchange's corporate governance rules require the audit committee of listed companies to discuss policies with respect to risk assessment and risk management. See Section 303A.07 of the NYSE Listed Company Manual.

[15] FINRA's predecessor issued a set of best practices for reviewing new products. While the notice applies to fund distributors, and not funds, it may be a useful resource. See NASD Notice to Members 05-26, *New Products: NASD Recommends Best Practices for Reviewing New Products* (April 2005).

[16] Segregation of functions, the independence of control groups, and exception and escalation procedures are discussed in *Risk Principles*, supra n. 4.

[17] See, e.g., Senior Supervisors Group, *Observations on Risk Management Practices During the Recent Market Turbulence* (March 6, 2008), listed in Additional Resources.

[18] See Rule 2a-7 under the 1940 Act.

[19] A "black swan" event is an unpredictable event with a significant impact. See Nassim Nicholas Taleb, *The Black Swan* (2007), which discusses various black swan events throughout history.

[20] See, e.g., COSO, *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks* (December 2010), listed in Additional Resources.

[21] Rule 38a-1 under the 1940 Act.

[22] The SEC's fund governance standards require the fund board to evaluate "at least once annually the performance of the board of directors and the committees of the board of directors, which evaluation must include a consideration of the effectiveness of the committee structure of the fund board and the number of funds on whose boards each director serves." SEC Rule 0-1(a)(7) under the 1940 Act.

[23] See n. 1, supra. For samples of disclosures added to fund registration statements in response to this new requirement, see ICI's report, *Disclosure of the Role of the Board in Risk Oversight, Samples of SAI Disclosure*, listed in Additional Resources.

Appendix A: Potential Board-Adviser Discussion Topics

Below is a list of topics and questions that a board might consider in connection with its oversight of risk management. These are not intended to reflect best practices or to be a model for boards to follow, nor are they intended to be comprehensive. Rather, the suggested topics are meant to assist boards in considering both the types of information they might seek and discuss with the adviser as well as matters to consider themselves when reviewing their risk oversight practices. Many boards may already be addressing these topics in their discussions, while others may determine that they are not applicable or helpful given the facts and circumstances of their particular fund and board.

Definitions and Risk Concepts

- How does the adviser define "risk," "risk management," and any other risk-related terms (see Appendix C) that are used in reports to and discussions with the board?
- If the term "enterprise risk management" is used, what is the "enterprise" that is referenced (for example, is it the adviser, its parent organization [including the adviser's affiliates], or does it include other service providers)?
- Does the adviser organize risks into any broad categories, such as investment risks and business operational risks?

Adviser's Risk Management Organizational Structure

- Where or with whom does the responsibility for risk management reside within the adviser?
- Does the adviser have a risk management oversight committee? If so, what is its composition and mandate?
- Does the adviser have any other committees with some responsibility for risk management, such as a new investments committee or a credit committee? If so, what are their compositions and mandates?
- Does the adviser have personnel whose core responsibility is risk management (such as a CRO or risk management professional staff)? If so, what are their respective:
  - responsibilities;
  - relevant experiences; and
  - reporting relationships within the adviser (or its parent organization)?
- Does the adviser have personnel who have risk management responsibilities in addition to other responsibilities (such as the CCO)? If so, what are their:
  - risk management responsibilities and the proportion of time devoted to this function;

- relevant experiences; and
- reporting relationships within the adviser (or its parent organization) regarding risk matters?

- How does the risk management function interface with other control functions, such as compliance (including the CCO), legal, and internal audit?
- Does the adviser or its parent company have a board of directors that oversees the adviser's risk management program? If so, what are:
  - the board's oversight processes;
  - the similarities with and differences between the reports the adviser's board receives as compared to those that the fund board receives; and
  - the processes for bringing to the fund board's attention any risk events or concerns affecting the fund that are discussed with the adviser's board?

Risk Management Processes

- Does the adviser use a risk assessment process to identify and measure risks? If so:
  - Who conducts the risk assessment?
  - What is the process and what is produced by the process (e.g., a risk matrix, a list of top risks)?
  - If applicable, how is each risk measured and by whom?
  - What types of qualitative measures are used (e.g., high, medium, low)?
  - How frequently is a risk assessment conducted?
  - What decisions are affected by risk assessments? For example:
    - Do risk assessments impact resource allocations?
    - Do risk assessments determine the type or timing of forensic testing that is done or any other risk-based tests?
- Does the adviser conduct stress tests or scenario analyses? If so:
  - What are the methodologies?
  - What were the results?
- What are the most significant risks to the fund?
  - What are the processes for mitigating, controlling, and monitoring those risks?
  - What are the criteria for prioritizing risks and who determines that criteria?
  - What is the status of any risk remediation plans that may be in place?

- What are the procedures, including criteria, for escalating significant risk-related matters, including risk events, to senior management, the adviser's board, and/or the fund board?
- Does the adviser's risk management process ensure the flow of information to senior management and key leaders in a timely and clear manner?
- Are sufficient resources and attention dedicated or allocated to the risk management function? Have these resources changed over the last year? If so, how and why?

Board Structure and Processes

- Is the board's committee structure effective for board oversight of risk management, given the size of the board, among other considerations?
- Are the mandates for each of the committees sufficiently clear with respect to any risk oversight responsibilities assigned to them?
- Should oversight of risk management be designated as a mandate that is assigned to a board committee?
- Are the board reports effective in informing the board of:
  - the risk management processes; and
  - the most significant risks to the funds?
- Should the frequency, format, or content of board reports be adjusted?
- Are there any particular risk topics on which the board would like an in-depth report, such as counterparty risk or business continuity?
- Does the board's counsel monitor relevant emerging risks that others in the industry may have identified and make the board aware of any such risks?

Specific Risk Topics

Investment Risks

- Regarding the persons who conduct investment risk analyses on the fund's portfolio:
  - What are their roles and reporting relationships within the adviser?
  - What are their backgrounds and expertise?
- What are the risks that the portfolio manager has to take to achieve the fund's performance results?
  - What are the nature and sources of the risks taken (e.g., equity market, interest rate, credit, leverage, liquidity, counterparty)?
- Is the portfolio manager's compensation structure designed to align his or her interests (and risk taking) with those of the fund's shareholders?

- What tools or analytics are used to monitor and manage risks?
- Are the benchmarks used for risk management purposes the same as for performance evaluation?
- Is there a process for evaluating a new type of investment's potential impact on portfolio management, operations, accounting, tax, and other functions before a fund invests in it?
- If a model is used to support portfolio management:
  - How many models are used in the investment process?
  - How is the model used (i.e., does it drive investment decisions or is it an input that is taken into account in investment decisions)?
  - What experience does the firm have with using the model?
  - If the model is developed by third parties, does the adviser sufficiently understand it?
  - Has the model performed as expected?
  - What are the criteria for revising the model's assumptions?
    - Are the assumptions used in the model still valid or do they need to be updated?
- How is counterparty risk tracked and managed?
  - Is counterparty exposure tracked and managed across all funds?

Middle- and Back-Office Operations

- Are there any significant customized or manual processes, such as for confirmations, settlements, and reconciliations? If so, what are the processes for assessing and controlling the operational risks associated with those processes?
- Does the adviser monitor any metrics or indicators to identify trends or early warnings of potential concerns, such as error or loss history reports or "near misses?"

Business Continuity

- What types of tests are conducted to evaluate the robustness of business continuity procedures?
- Has consideration been given to the business impact of widespread disruptions of basic services such as electricity and water supplies?

Information Technology and Security

- What types of tests are conducted to evaluate the robustness of information technology security and for protecting material, nonpublic information?
- Have there been any recent significant breaches or disruptions in service?
- How does the adviser stay current on threats to data privacy (such as hacking threats)?
- When and how are the risks associated with introducing a new information technology system evaluated?

Physical Security

- Who is responsible for maintaining office security and what procedures are in place to escalate any concerns to senior management?
- What steps have been taken to protect the physical security of locations and employees (e.g., mail bomb threats)?

Human Capital

- Does the adviser have succession plans in place for key professionals?
- What are some of the personnel policies that help mitigate reputational risk to the fund?

Other Service Providers

- How do the adviser and other service providers (e.g., custodian, transfer agent) interface with respect to the management of risks impacting the fund?
- When and how are the risks associated with bringing on a new service provider evaluated?

Legal/Regulatory Compliance

- What litigation risks does the fund have?
- How does the fund's CCO prioritize regulatory and compliance risks presented to the fund by its adviser and service providers?
- What operational or other risks are presented by the implementation of new regulatory requirements?
- What processes are in place to ensure that the fund's investment risks are adequately disclosed in the fund's registration statement?
- What processes are in place to ensure that sales and marketing communications are consistent with the fund's registration statement?
- What procedures are in place to ensure the fund's net asset value is accurately calculated on time each business day?

Appendix B: Discussion of Investment Risk Management Practices

To achieve investment returns, a fund must incur investment risks. The goal of investment risk management is to ensure that those risks are understood, intended, and compensated.

What is Investment Risk?

There is a spectrum of perspectives on investment risk. At one end, it may be viewed in absolute terms as the risk of incurring any loss in a portfolio, whether on a daily basis or upon redemption from the fund. At the other end, it may be viewed in relative terms as the risk that the fund will incur losses greater than, or earn gains less than, those of a benchmark index or alternative investment. In practice, investment professionals' views of risk generally are a blend of these two perspectives. A board may want to discuss with the adviser (and its portfolio and risk management teams) how it views and measures the fund's risks.

Investment Risk Management Practices

Investment risk management should be based on reasonable investor expectations about the risks that the fund will take in order to achieve its investment objectives, which can be thought of as the fund's risk profile or risk appetite. A fund's risk profile is found in and arises from its communications with investors—its prospectus, Statement of Additional Information (SAI), and marketing materials—which state the fund's investment strategies and risk factors. The risk profile consists of both restrictive rules and affirmative principles. The restrictive rules serve as "guardrails" that place absolute limits on the sources and levels of risk that the adviser can take to be consistent with the fund's investment objective and strategies. All funds are subject to some limits by regulation (e.g., borrowing and leverage). In addition, funds may restrict their exposure to certain asset classes (e.g., commodities, real estate, certain types of securitizations, or assets with low credit ratings) and may limit short selling and/or the use of derivatives. The fund's stated objectives, strategies, and marketing materials express the principles regarding the amount of risk that the adviser can take to be consistent with the mandate. For example, a fund that has the primary objective of preservation of capital, that states it will primarily seek to attain this objective through purchasing short-term bonds, and that is marketed as a conservative investment will have a low investment risk profile; in contrast, a fund that seeks aggressive growth of capital, that states that it will invest in early-stage companies, and that is marketed as a long-term investment will have a higher investment risk profile.

Risk Control and Management

Investment risk management involves both controlling risk by limiting certain risk exposures, and thus the size and probability of losses, as well as using a number of active investment techniques that seek to align the fund's investments with its investment objectives, its risk profile, and the portfolio manager's investment convictions.

Risk control is focused on placing limits on a fund's investment positions and concentrations. These limits include the investment restrictions in the fund's prospectus and SAI as well as any limits and restrictions imposed by the investment team. Risk control activities may include reviewing portfolio concentrations and adjusting portfolio holdings accordingly; evaluating and reviewing new and/or complex instruments, such as derivatives, and imposing conditions and limits on their use; monitoring and limiting credit exposure from issuers of portfolio securities and from counterparties; and ensuring that a fund is managed in compliance with any prospectus/SAI/regulatory investment restrictions.

Active risk management is premised on the insight that all investment decisions involve a series of trade-offs between the potential for returns and certain risks. It seeks to ensure that the risks resulting from investment decisions are understood, intended, compensated, and aligned with the affirmative principles of the fund's investment objectives and strategies.

Portfolio Management Evaluation and Support

Regardless of whether an adviser has dedicated portfolio risk management personnel, risk management is a distinct function that plays two key, interrelated roles: it evaluates the portfolio's risk exposures and supports the portfolio managers in performing their risk management function. For instance, risk managers may provide a top-down, quantitative view of the risks in each fund portfolio, which can contrast with and provide a different view of risk than the fundamental, bottom-up, security-by-security analysis performed by many portfolio managers. For portfolio managers that use quantitative models, risk managers can test the assumptions, inputs, and data on which the model is built. The combination of these two perspectives can help portfolio managers and senior management gain a better understanding of a fund's investment risks.

Risk managers may provide regular risk reports to portfolio managers, which may include reviews of portfolio industry, country, and sector weightings against those of the fund's benchmarks; analyses of the portfolio's exposure to risk factors using risk models based on historical price relationships; and stress testing and "tail" risk analysis. The frequency of reports may depend on the type of fund and frequency with which the fund's exposures may change. For example, because the risk metrics for a fixed income fund may change more frequently than those of an equity fund with low portfolio turnover, risk managers may provide reports to the fixed income manager more frequently (e.g., daily) than to the equity manager (e.g., monthly). Risk managers also may assist portfolio managers in setting risk "budgets" for a fund. Risk budgeting involves breaking down investment risk into its components or drivers, setting limits on each, and allocating holdings to reflect these limits. Risk managers also can offer expertise in constructing and testing financial models to portfolio managers.

Analytical Tools and Metrics

Risk managers make use of a range of analytical tests, tools, and metrics in their analyses and reports. Because no one test provides all necessary information, risk managers typically use a variety of metrics, many of which are based on a defined benchmark or index. Consistency in the use of benchmarks and methodologies for purposes of risk analyses and performance evaluation is key to comparability of analyses through time and across funds. Risk managers typically combine backward- and forward-looking analyses. Backward-looking metrics, such as tracking error against an index, have the advantage of quantitative precision, because they typically are based on robust historical data. However, as many risk managers discovered during the financial crisis of 2007–2009, these data sets have their flaws and limitations, and markets do not always behave as they have in the past. Forward-looking analyses, such as stress testing and scenario analyses, are designed to address this weakness by building assumptions about negative events and scenarios into risk models; however, these assumptions also may be based on historical performance, and they may prove to be incorrect.

Some of the most common quantitative risk metrics include:

- *Standard deviation*—a measure of the variability of a data set (including a data set of investment returns). A low standard deviation indicates that the data points tend to be very close to the same value (the mean), while high standard deviation indicates that the data are spread out over a large range of values.
- *Value-at-Risk (VaR)*—the maximum loss in cash terms over a finite period (e.g., one day or one month) given a certain level of confidence (such as 99 percent or 95 percent). VaR is best understood in terms of the bell curve or "normal" distribution: VaR focuses on the outcomes at the curve's left tail, two or three standard deviations from the mean. VaR also may be based on historical information and, thus, has its limitations.
- *Sharpe ratio*—a measure of an investment's risk-adjusted returns. It is calculated by dividing an investment's returns in excess of the risk-free rate (i.e., Treasury bill rates) by the investment's standard deviation. Positive values indicate that a manager is generating incremental returns for the risk they have taken on. Negative values indicate a manager has underperformed the risk-free rate.
- *Information ratio*—an assessment of the value generated by active management of the portfolio. It is calculated by subtracting the benchmark return from the portfolio return and dividing by the tracking error. A manager that did not add value would be expected to have an information ratio of zero. Any information ratio above zero means that the portfolio manager has outperformed the benchmark and has not taken undue risks relative to that index.

» *Stress tests*—a range of techniques used to assess the vulnerability of a portfolio to exceptional but plausible shocks. Stress testing involves constructing models of portfolio performance and analyzing the effects of scenarios such as a certain percentage decrease in an equity index's value or increase in interest rates. Stress testing under a wider range of scenarios can provide particular insights into the robustness of quantitative investment models.

Since the failure of Lehman Brothers, counterparty credit risk has gained particular attention at many fund advisers. For funds that use OTC derivatives, the failure of a counterparty could result in losses, and the financial weakness of the counterparty might not be apparent until failure is near. Therefore, many advisers subject their funds' counterparties to the same type of credit analysis applicable to fixed income investments. Such credit analysis can include quantitative measures of financial strength such as capital and leverage ratios, as well as market-based measures, such as the price of the firm's subordinated debt or the price of purchasing default protection on such debt through credit derivatives.

Who Performs Investment Risk Management

Many advisers have a process for providing independent risk analyses of their funds' portfolios. Some advisers have a team of risk analysts (either within the portfolio management group or in a separate group with different reporting lines) that generates analyses of fund portfolios. Advisers without dedicated risk analysts may rely on peer reviews or the CIO to separately evaluate the fund's risks. There is no single "right" way to organize investment risk management; the complexity and range of the risks to be managed, the techniques used, and the adviser's particular collection of talent, size, and history will drive the organizational structure.

Whatever the structure, an appropriate degree of independence enhances the effectiveness of risk management. An independent and different perspective can help portfolio managers test the premises and assumptions behind their investment decisions and provide insights that the portfolio managers might have missed or discounted. A review that is independent of portfolio management also can serve as a check against any inadvertent or excessive risk-taking by the portfolio manager. Nonetheless, risk management also should be integrated with and collaborate with portfolio management so that they have each other's trust. In a healthy risk management process, portfolio management and risk management form a robust feedback loop in which investment positions and returns are analyzed for risk, and risk reports and model evaluations inform an investment process that provides better risk-adjusted returns.

Supporting Fund Board Oversight

Fund boards have heightened their focus on investment risk since the financial crisis, and a noteworthy trend has been the increasing quantity and complexity of reporting by risk management personnel to fund boards. Some boards regularly meet with risk managers in executive session or receive risk presentations from them during board meetings, and a number of boards also receive written risk reports in board meeting materials. Risk and performance reports are central to a board's investment oversight responsibilities. The content and formats of these reports vary with the board, the fund, and the adviser, and the starting point will likely be the adviser's own risk reporting. Risk reports either can be stand-alone documents or integrated with performance reporting. They can encompass a range of different approaches, including a single-page "dashboard" of key metrics in tables or graphs, qualitative summaries of risks and controls, regular attribution analysis, and more specialized reports such as trends analysis or exception reports.

Risk managers also may assist the board in fulfilling its oversight function by educating the board about investment risks and risk management techniques and tools, either in the regular course of board meetings or in special sessions.

Appendix C: Common Risk Terms

The following are terms that may arise in board reports or board discussions with the adviser about risk management. Boards and advisers may establish different definitions for these terms.

counterparty risk. The risk associated with the financial stability of the opposite party of a contract, such as a swap.

credit risk. The possibility that an issuer of a bond will default by failing to repay principal and/or interest in a timely manner.

enterprise risk management. A process, effected or overseen by an entity's board of directors, management, and/or other personnel that is applied across the enterprise to: set risk strategies; identify potential events that may affect the entity; ensure that risks are managed to be within the enterprise's risk appetite; and provide reasonable assurance regarding the achievement of objectives.

information ratio. An assessment of the value generated by active management of the portfolio. It is calculated by subtracting the benchmark return from the portfolio return and dividing by the tracking error. A manager that did not add value would be expected to have an information ratio of zero. Any information ratio above zero means that the portfolio manager has outperformed the benchmark and has not taken undue risks relative to that index.

interest rate risk. The risk that a security's value will change due to a change in interest rates.

investment risk. In absolute terms, it is the risk of incurring any loss in the portfolio in pursuit of investment return; in relative terms, it is the risk of incurring losses greater than, or of earning gains less than, those of a benchmark index or alternative investment.

key risk indicators (KRIs). Metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.

market risk. Risk resulting from movements in market prices, including changes in interest rates, foreign exchange rates, volatilities, and equity and commodity prices.

operational risk. The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

risk. In a narrow sense, the possibility of loss or a bad outcome; in a broader sense, a neutral measure of the degree to which uncertainty exists about the outcome of an action.

risk appetite. The amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value.

risk assessment. The process of identifying and analyzing risks, considering their likelihood and impact.

risk budgeting. A risk management technique in which assets are allocated efficiently so that the expected return of each asset is proportional to its contribution to portfolio risk.

risk inventory. A collection of risks, with assigned ranking, produced by a risk assessment.

risk management. The process of identifying, assessing, and controlling both enterprise and portfolio risks in order to minimize unanticipated losses and uncompensated risks and optimize the reward/risk ratio.

Sharpe ratio. A measure of an investment's risk-adjusted returns. It is calculated by dividing an investment's returns in excess of the risk-free rate (i.e., Treasury bill rates) by the investment's standard deviation. Positive values indicate that a manager is generating incremental returns for the risk they have taken on. Negative values indicate a manager has underperformed the risk-free rate.

standard deviation. A measure of the variability of a data set (including a data set of investment returns). A low standard deviation indicates that the data points tend to be very close to the same value (the mean), while high standard deviation indicates that the data are spread out over a large range of values.

value-at-risk (VaR). The maximum loss in cash terms over a finite period (e.g., one day or one month) given a certain level of confidence (such as 99 percent or 95 percent). VaR is best understood in terms of the bell curve or "normal" distribution: VaR focuses on the outcomes at the curve's left tail, two or three standard deviations from the mean.

Additional Resources

The following websites and publications contain additional information related to risk management. They are merely a sample of a large number of available sources. Except for the ICI and IDC websites and publications, the websites and publications listed below are created, maintained, and published by other organizations. ICI and IDC do not control, cannot guarantee, and are not responsible for the accuracy, timeliness, or even the continued availability of this outside information. By listing these references, ICI and IDC also do not purport to endorse the organizations or their statements.

Publications

ICI and IDC Publications

- *Disclosure of the Role of the Board in Risk Oversight, Samples of SAI Disclosure* (October 2010)
  www.ici.org/pdf/ppr_10_risk_disclosure.pdf
- *Chief Risk Officers in the Mutual Fund Industry: Who Are They and What is Their Role Within the Organization?* (August 2007)
  www.ici.org/pdf/21437.pdf
- *Fair Valuation Series: An Introduction to Fair Valuation* (June 2005)
  www.idc.org/pdf/05_fair_valuation_intro.pdf
- *Fair Valuation Series: The Role of the Board* (January 2006)
  www.idc.org/pdf/06_fair_valuation_board.pdf
- *Board Oversight of Fund Compliance* (September 2009)
  www.idc.org/pdf/idc_09_compliance.pdf
- *Board Oversight of Derivatives* (July 2008)
  www.idc.org/pdf/ppr_08_derivatives.pdf
- *Board Oversight of Subadvisers* (July 2010)
  www.idc.org/pdf/idc_10_subadvisers.pdf
- *Board Oversight of Certain Service Providers* (June 2007)
  www.idc.org/pdf/21229.pdf

Buy Side Risk Managers Forum and Capital Market Risk Advisors Publication

- Risk Principles for Asset Managers (February 2008)
  www.buysiderisk.org/20080129%20Risk%20Principles.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Publications

- *Board Risk Oversight: Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities* (December 2010) www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf
- *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks* (December 2010) www.coso.org/documents/COSOKRIPaperFull-FINALforWebPostingDec110_000.pdf
- *Effective Enterprise Risk Oversight: The Role of the Board of Directors* (August 2009) www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf
- *Enterprise Risk Management—Integrated Framework* (September 2004) www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp

Senior Supervisors Group (SSG) Publications

- *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure* (December 2010) www.ny.frb.org/newsevents/news/banking/2010/an101223.pdf.
- *Risk Management Lessons from the Global Banking Crisis of 2008* (October 2009) www.sec.gov/news/press/2009/report102109.pdf
- *Observations on Risk Management Practices During the Recent Market Turbulence* (March 2008) www.sec.gov/news/press/2008/report030608.pdf.

Deloitte & Touche LLP Publications

- *Risk Intelligent Governance; A Practical Guide for Boards* (2009) www.deloitte.com/view/en_US/us/Services/audit-enterprise-risk-services/governance-regulatory-risk-strategies/Enterprise-Risk-Management/f90626eb72034210VgnVCM100000ba42f00aRCRD.htm
- *Risk Intelligent Enterprise Management: Running the Risk Intelligent Enterprise™* (2010) www.deloitte.com/view/en_US/us/Services/deloitte-growth-enterprise-services/deloitte-growth-enterprise-services-organizational-transformation/70cadc11335ec210VgnVCM3000001c56f00aRCRD.htm.

PricewaterhouseCoopers LLP Publications

» *Cure for the Common Culture: Building Effective Risk Cultures at Financial Institutions* (April 2011) www.pwc.com/en_US/us/financial-services/forms/viewpoint-cure-for-the-common-culture.jhtml.

The Investment Company Institute (ICI) is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds (ETFs), and unit investment trusts (UITs). ICI seeks to encourage adherence to high ethical standards by all industry participants; advance the interests of funds, their shareholders, directors, and advisers; and promote public understanding of mutual funds and other investment companies.

INDEPENDENT DIRECTORS COUNCIL

The Independent Directors Council (IDC) serves the fund independent director community and provides a venue to advance the education, interaction, communication, and policy positions of fund independent directors.

1401 H Street, NW, Washington, DC 20005-2148 202/326-5800