Deloitte.

MFDF
Trusted Insight for Independent Oversight

Role of the fund director in the oversight of the risk management function

April 2025

Contents

Foreword

Since the Role of the Mutual Fund Director in the Oversight of the Risk Management Function[1] (the Risk Paper) was last published in 2022, the world has changed drastically. Fund complexes have faced new challenges and opportunities as a result. In addition to evergreen risks the fund industry faces, this paper highlights emerging risks facing fund complexes, including new regulations; new investment opportunities; and evolving technology and tools, such as the increasing focus on artificial intelligence. Artificial intelligence is being thought of as a solution for a wide range of fund business activities, not just investments.

The paper lays out questions directors may wish to consider in their risk oversight role. While each organization faces different risks and has its own unique risk management frameworks and programs, this paper can serve as a guide to help directors in the face of the ever-evolving risk landscape.

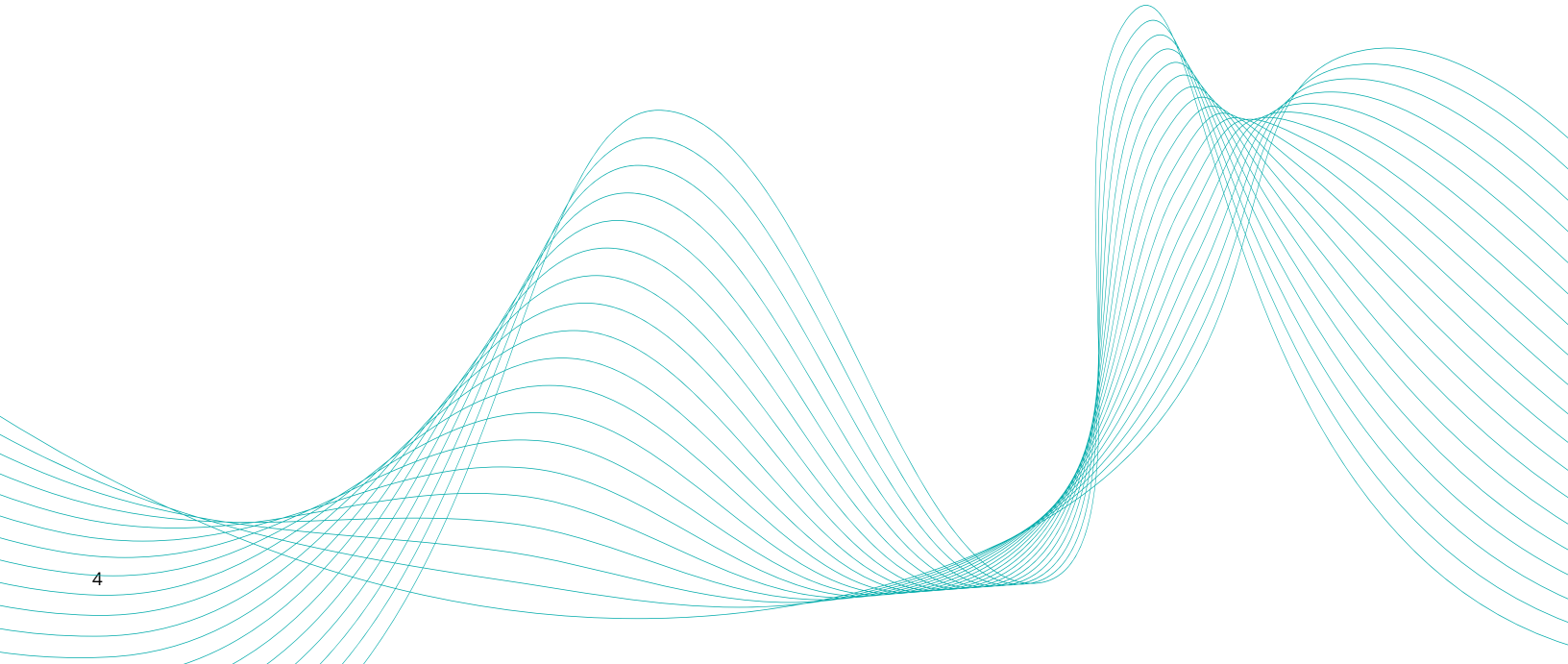
Introduction

Boards of registered funds (hereafter referred to as fund directors, directors, fund boards, or boards) have an important role in risk oversight. In considering their oversight responsibilities, directors may find it helpful to distinguish between risks that are inherent in the fund's investment strategy and other risks that are unexpected. An open, ongoing, transparent dialogue among the directors, adviser, and other key service providers is important to supporting board risk oversight.

This paper[2] sets forth key concepts, principles, and some initial questions that fund directors may find useful as they seek more information to support their risk oversight responsibilities. This paper builds and expands upon the previous May 2022 paper, noting where enhanced or new content has been provided. As with the earlier paper:

- The first section lays out a fund director's role and duties.
- The second section sets forth common risk management program elements and practices to help fund directors better understand how investment advisers and service providers manage risks to the funds they oversee.
- The final section discusses specific areas of existing, evolving, and emerging risks that impact the investment management industry.

The MFDF recognizes that a "one-size-fits all" approach to risk oversight and risk programs is not feasible nor beneficial. Consequently, when discussing funds' risks and the programs designed to manage those risks, directors should consider the factors relevant to their particular funds, such as each fund's investment objective, asset size, and complexity. Importantly, fund directors should also be aware of whether their fund's adviser and other key service providers have appropriate risk management programs and practices in place for identifying, analyzing, managing, and reporting existing, evolving, and emerging material fund risks across all risk categories.



Roles and duties of fund directors

Fund directors are responsible for general understanding of, and overseeing how, the fund's adviser manages a fund's risk. While there are no regulatory-defined duties with respect to risk for fund directors, fund directors can establish a solid foundation for risk oversight by developing an understanding of the:

- Obligations arising under state law, the Investment Company Act of 1940 (1940 Act) and the Securities Act of 1933 (1933 Act)
- Applicable guidance from courts and the Securities and Exchange Commission (SEC) and its staff regarding their expectations for directors
- Most significant strategic, investment, operational, regulatory, and emerging risks affecting a fund and fund complex, and
- Risk management programs and processes implemented by the adviser to identify, manage, and mitigate risk. Directors may look to the adviser to monitor the risk management programs and process implemented by service providers.

Obligations under state law, the 1940 Act, and the 1933 Act

Funds are organized under state laws and, as a result, a director is considered a fiduciary to the fund.[3] As a fiduciary, a director owes two basic duties to the fund: the "duty of care" and the "duty of loyalty."

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

In assessing the actions of directors, courts apply the "business judgment rule," which insulates a director from liability for a business decision made in good faith if: (i) the director is not interested in the subject of the business decision; (ii) is sufficiently informed to make the business decision; and (iii) rationally believes that the business decision is in the best interests of the company.[4]

In addition to state law fiduciary duties, the 1940 Act and its regulations, together with SEC statements, also impose duties on directors in three general areas:

- Evaluating fees charged to the fund and valuing the fund's assets,[5]
- Dealing with conflicts of interest,[6] and
- Assessing key third-party service providers,[7] including initial and ongoing due diligence.

Lastly, the 1933 Act also imposes certain legal duties on fund directors with respect to registration statements, requiring a majority of the board to sign the registration statement of a fund prior to its filing and imposing individual liability for any untrue statement of material fact or material omission in the registration statement.[8]

Court and SEC guidance

The US Supreme Court, SEC, and SEC staff have consistently emphasized that the fundamental obligation of a fund director is to protect the interests of a fund's investors.

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

- Request information regarding the fund's activities and the critical services provided to the fund to enable directors to develop an appropriate appreciation of the risks inherent in the operation of a fund and to then assess the effectiveness of risk practices and controls implemented by the adviser and other service providers.
- Receive regular updates regarding the risks associated with outsourced services and how they are being managed by the adviser or appropriate service provider, and other parties within the extended enterprise.
- Evaluate on an ongoing basis whether fund policies and procedures are reasonably designed and operating effectively to prevent the fund's operations from violating applicable federal securities laws.[9]

While fund directors could be tempted to become drawn into the day-to-day operations of a fund, a fund director's primary responsibility is to provide oversight and operate as an independent check on those charged with day-to-day management of the fund's activities.[10]

Fund directors should work with the fund's investment adviser and service providers and consult with outside experts—as applicable—to understand and oversee how risks are identified, assessed, and managed. In addition to consulting with the adviser's risk management personnel, the fund's chief compliance officer (CCO) can be a significant resource for boards in overseeing risk management effectively. While the CCO is not responsible for managing risks, the CCO may learn valuable information about operational and other risks as part of the administration of the fund's compliance program. Understanding the relevant scope, plans, and outcomes of the adviser's internal audit function and other integrated business functions can facilitate the board's oversight responsibilities.

The risk management framework and program

As outlined in the introduction, effective risk management is not a one-size-fits-all exercise and should be tailored to the fund and fund complex's size, structure, and other relevant attributes. While fund directors are not responsible for risk management, they should understand the adviser's risk framework, the program for risk identification, assessment, mitigation, monitoring, and reporting. Fund directors should evaluate how the adviser tailors its risk management program to address the existing risks it faces, as well as to emerging risks. Although fund directors are not responsible for day-to-day management of these risks, they hold a crucial responsibility for overseeing the risk management process within the entities they govern.

Despite the diversity in how risk management programs and practices may be designed and implemented, most risk management programs follow a similar approach and principles. Risk management programs should be designed to identify, measure, and manage the most significant risks to within an acceptable risk appetite or tolerance level, not eliminate or fully mitigate every risk. Moreover, as advisers grow, their product offerings and business operations evolve, and external factors change (e.g., regulatory environment), their risk management programs should adapt to these changes as well.

Regardless of the particular risk management program or model that is used by the adviser and other service providers, there are significant elements and processes that are typically included in an effective risk management program as discussed in more detail in the following sections.

Risks evolve over time and vary depending on the fund's particular facts and circumstances, such as the fund's investment objective, principal strategies; its internal operating environment including outsourced service providers; and external forces such as industry and regulatory changes. In general, risk can be broadly divided into five categories:

An effective risk management framework and program allows the adviser and other service providers to identify and manage risks that are relevant to a particular fund and fund complex.

Investment risks (page 11), which are risks related to a fund's portfolio composition, including but not limited to market, credit, liquidity, derivatives, and leverage risks.

Technology risks (page 16), which are risks related to information technology, cloud, cybersecurity, data, models, and artificial intelligence.

Operational risks (page 19), which include risks related to day-to-day operations, business resilience, and third-party provider risk.

Regulatory risks (page 21), which are related to regulatory changes and guidance and how regulations are interpreted and implemented as well as compliance with various existing regulations.

Strategic risks (page 23), which are those that could disrupt the objectives and assumptions that define an adviser's business strategy, including risks to competitive position, reputation, and strategy execution.

Elements of an effective risk management program

Governance, tone at the top, and risk culture

Good governance is essential to an effective risk management program, and good governance starts with the attitudes and principles of those in the most senior positions at an adviser or service provider.[11] These attitudes and principles are referred to as "tone at the top" and should cascade throughout the firm. This should become the tone throughout the organization and be embedded as a fundamental principle and belief that risk is everyone's responsibility. The tone at the top along with these embedded beliefs help define a firm's risk culture.

Thus, the "tone at the top" is important to understand when considering the adviser or other critical service provider's risk philosophy and approach to risk management. While the tone at the top may be difficult to evaluate empirically, fund directors can gain insight by engaging in discussions with senior management, as well as external auditors and outside counsel, to help understand and appreciate the tone at the top and overall risk culture. Directors may look to the adviser for its assessment of the culture at other critical service providers.

In further evaluating the risk culture at a firm, a fund director may find it helpful to determine how the risk management program of the adviser operates, which can be facilitated by meeting with key risk management personnel. In doing so, fund directors may find the following questions helpful to consider:

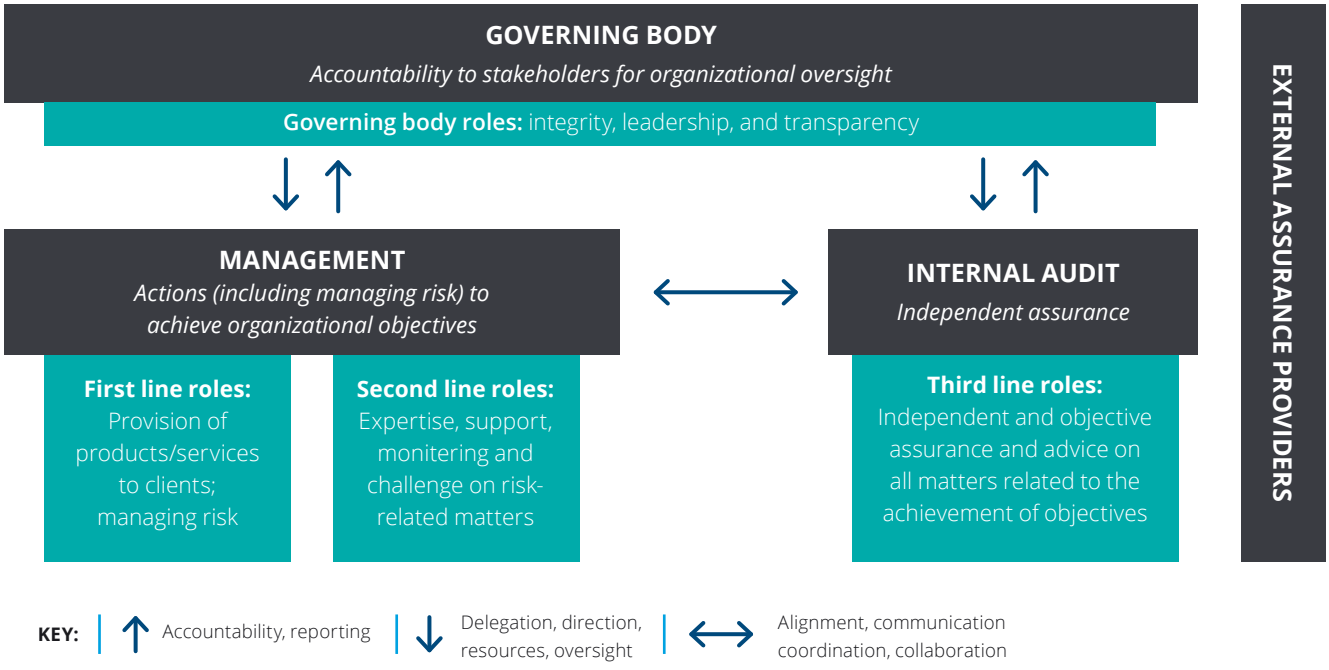
- Who is responsible for overall risk management and what is the governance structure? Is there an enterprise-wide risk management committee or other governing body?
- Are risk manager roles within business units or outside of them, or both? Are there well-defined first- and second-line risk roles and responsibilities?
- What is the process for identifying and monitoring existing, evolving, and emerging risks? How is ongoing risk monitoring performed?
- Is there an understanding between the adviser and the board as to what type of risks should be escalated and discussed?
- How are key risks determined, agreed upon, or ratified? How are key risks—and the process, controls, and plans to mitigate these risks—monitored, reported, and challenged within the organization?
- How does the adviser encourage an appropriate risk culture? How does the adviser incentivize appropriate risk-taking (and not incentivize inappropriate risk-taking)?

The Three Lines Model for good risk governance

It is also important for fund directors to understand how roles and responsibilities for executing the risk and control processes have been delineated in the adviser's organization. In many organizations, different teams have risk management responsibilities, including enterprise, operational, and investment risk professionals; compliance officers; internal audit professionals; control assurance specialists; and other risk and control professionals who are embedded in or supporting the business. These teams each have a unique perspective and role but are collectively working together to help the adviser manage and evaluate risk. While every adviser is unique and, as a result, there is no single or right way to organize risk functions, responsibilities should be clearly delineated and understood, and the work coordinated when possible and practicable.

One commonly used framework for defining roles and responsibilities is the Institute of Internal Auditors' (IIA) Three Lines Model. In this model, the first line is responsible for risk identification and mitigation, the second line provides support, challenge, and risk monitoring capabilities, and the third line provides independent assurance. Each of these three lines plays a distinct role within the organization's wider governance framework. The fund's CCO should also have a direct line to the board (the "governing body" in the model in figure 1[12]). When applicable, the chief internal audit executive, who typically reports to the board of the adviser or an affiliated entity, could also present to the fund's board.

Figure 1. The IIA's Three Lines Model[13]



Risk communication and reporting

When evaluating the appropriateness and sufficiency of risk-related communications and reporting, the board may wish to consider:

- The adviser's and/or service provider's communication of risk management protocols and expectations, including those related to risk event escalation and reporting, to all those involved; and
- Ongoing risk-related reporting.

The board can work with the adviser to develop reporting to support the fund board's understanding of the adviser's risk management program and its oversight of key service providers' risks, as well as ongoing fund-related risk reporting (e.g., key risks and key risk indicators, or KRIs). Such reporting helps the board understand the adviser's and service provider's current risk management programs and how well they are managing the risks to the funds.

In addition to the reporting and communications the fund board receives, directors should examine how the board structures and addresses its risk oversight responsibilities, and to determine it has the right level of dialog with the adviser relating to strategic risks facing the organization. For example, some boards may find it helpful to have a board risk committee, whereas others prefer to address risk as part of another committee's responsibility (e.g., audit or compliance) and still others have risk remain at the full board level. This decision will impact how the board interacts with the adviser and service providers and sets expectations for ongoing risk-related reporting, communication, and discussions.

As fund directors consider their expected risk-related communications and reporting, the following questions may be helpful:

- How often should the adviser and service providers review and discuss their risk management processes with the fund board? Who is responsible for these discussions? Does this reporting provide the directors with an appropriate level of visibility into the risk management program and how it is functioning?
- What is the current risk and risk management-related reporting to fund directors? Does the current risk reporting meet director expectations?
- How is the reporting reviewed and discussed? How does this risk reporting compare to the reporting received by the risk management governing bodies of the adviser or service provider (e.g., enterprise-wide risk committee)?
- What are the current gaps in the risk management process and what is the adviser's remediation plan?

Risk identification and assessment

The adviser's risk management program should include a process to timely identify and assess risks. Understanding the risk identification and assessment processes of an adviser and other service providers is an important aspect of the overall risk program. While there are no standardized approaches to identify and assess risk, there are some common principles such as understanding organizational objectives and supporting end-to-end processes and underlying people, processes, and technology that may contribute to the risk that an organization faces.

To understand risk identification and assessment, fund directors may find it helpful to raise the following questions:

- What is the adviser's approach to identifying and assessing risk?
- How frequently does the adviser undertake such risk identification and assessment activities?
- Who is typically involved in the risk identification and assessment process?
- What happens when there are changes to the organization, processes, people, or technology, and how is that factored into the risk identification and assessment process?
- Are there any tools utilized to enable and/or facilitate the risk identification and assessment process?
- What is the process to review and approve the results of the risk identification and assessment?
- What technology applications are applied to the identification of risks?

Risk appetite and risk tolerances

Risk appetite is defined as the amount of risk, on a broad level, an entity is willing to accept as it tries to achieve its goal and provide value to stakeholders. Risk tolerance is the acceptable level of variation relative to achievement of a specific objective.[14]

Within an adviser, risk appetite and related risk tolerances set expectations for acceptable variations of risks across the fund complex to monitor actual risk levels as compared to the established tolerances around specific objectives. Establishing and using risk tolerances to monitor risk can allow the adviser to better understand, manage, and monitor whether the risks are in line with the adviser's business strategy, fund's objectives, and the expectations of its shareholders.

Understanding the risk appetite of an adviser or other significant service provider, however, can be challenging due to the highly subjective nature of identifying and articulating risk appetite across an entire organization and the varied approaches to defining and monitoring risk tolerances. There are no common standards, and different advisers may use different methodologies, language, and metrics (e.g., KRIs), which can be both qualitative and quantitative or some mix of both.

To understand risk appetite and related risk tolerances, fund directors may find it helpful to raise the following questions:

- What is the adviser's approach to defining risk appetite, and how is risk appetite used to monitor overall levels of risk?
- Are risk tolerances or risk thresholds established to monitor risk levels, and—if so—how?
- How are actual levels and/or key risks measured against the risk appetite? If KRIs are used, how are they defined and reported?
- What happens if a particular level or key risk is out of tolerance? And if multiple risks are out of tolerance?
- How is the overall, firmwide level of risk monitored in comparison to risk appetite?
- How often are risk appetite statements and/or risk tolerances reviewed?
- What is the process to review and approve changes to risk appetite statements and/or related risk tolerances?
- Is there alignment between the organization's top-level risks and the risk appetite statements at the operating unit level of the business?

Risk events and incidents

Risk events or incidents can include information security or cyber breaches; investment guideline or restriction breaches; trading, pricing, or valuation errors; or other incidents affecting the fund or its shareholders. Understanding the adviser's (as well as other service providers') risk event or incident management process is important to the board's risk oversight and beneficial to understanding how risk is managed in an ongoing, day-to-day business.

Immediately following the identification of a risk event or incident, an adviser should focus on correction and/or remediation to eliminate or minimize harm to the fund(s) or shareholders. Subsequently, the adviser should have an in-depth process for identifying the root cause of the incident as an important step in preventing future occurrence. Once the root cause (or sometimes multiple causes) for the incident has been determined, the adviser can then focus on preventing recurrence in the future.

Fund boards should understand the policies, procedures, and reporting in place to fully oversee this end-to-end process. Boards also should understand how the adviser and service providers seek to prevent reoccurrence in the future.

As boards consider the incident management program and process at the adviser, the questions below may be helpful:

- How are incidents timely identified, escalated, managed, and remediated?
- What is the process for understanding the root cause, or causes, and how to prevent them in the future?
- How and to whom are incidents escalated to ensure appropriate response and awareness? Under what circumstances are the board notified of incidents?
- How are risk events and incidents considered in the identification and assessment of a potential broader risk occurrence within the business?
- What specific reporting should the fund board receive to fully understand the process and impacts to the fund?

Risk mitigation strategies and control activities

Control activities are actions (generally described in policies, procedures, and standards) that help management mitigate risks. Control activities may be preventive or detective in nature and may be performed at all levels of the organization. They include management-level controls and internal controls in the business processes and activities as well as those performed by oversight functions (e.g., financial controls, risk management, compliance).

It may be helpful for a board to understand how each responsible party supports the control structure with respect to how controls are developed, maintained, and assessed in the normal course as well as how controls are adapted as risks evolve.

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

- How does the adviser manage and develop controls to mitigate risks?
- How does the culture of the adviser enable the risk management process?
- How does the adviser assess the effectiveness of controls? Is there strong coordination and collaboration between the various risk and assurance functions (see next section)? How are the results of such assessments communicated to the board?
- What is the role of the internal audit function in testing and reporting on control activities? How is the audit plan developed? Does the plan align to key risks? Does internal audit have agile processes in place to respond to emerging risks?
- How are emerging risks integrated into the control structure? For example, how has the remote working environment influenced the design of new or modified controls?
- Does the adviser monitor automated control activities differently from those that rely on more manual processes? If so, how does the monitoring differ?
- Does the adviser leverage artificial intelligence through automation (e.g., robotic process automation) and/or cognitive technologies (e.g., machine learning, natural language processing) to perform more intelligent testing/ continuous monitoring of controls?
- Does the adviser engage with third-party subject-matter specialists to support assessing/monitoring specific risks that may benefit from subject matter expertise?

Benefits of risk and assurance alignment and integration

As advisers and service providers plan and execute risk management and assurance activities, frequent coordination and collaboration among risk and assurance functions is necessary. As functions throughout the business address the various risks facing their line of business, there is a chance of risk reporting becoming siloed, leading to redundancies and extra costs. For particularly complex organizations, integrated assurance can help prevent some of these redundancies.

At a minimum, an organization should ensure alignment across the functions, including thoughtful planning, an understanding of cross functional responsibilities, addressing any unhelpful overlap of risk and assurance activities, and coordinated scheduling of assurance activities. Cross functional considerations should be woven into the execution cycle with frequent, meaningful discussions around themes and insights. As an example, risk themes should be collectively considered by risk and assurance functions during the reporting cycle.

As a next step, some organizations are moving past alignment to adopt a more integrated risk and assurance model anchored in (1) identifying drivers of business value, (2) understanding risks associated with delivering business value, and (3) aligning risk monitoring, reporting, and related assurance activities around these risks.

Together, these practices provide the building blocks to implementing both a holistic and tailored integrated risk and assurance model.

Risk framework and program evaluation

An adviser should continuously evaluate its risk management framework and program to keep pace with the evolving business, shareholder expectations, market conditions, and regulatory focus. Chief risk officers (CROs), or other appropriate risk management leaders, may provide insights to fund boards as to how and how often the organization evaluates the risk management framework and program and what actions are taken in response.

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

- How effective has the risk management program been in reducing risks?
- Does the risk management program incorporate effective mitigating controls? How do the risk leaders determine whether a risk program has been effective?
- What has been learned from risk failures and how is the adviser responding?

Adaptive risk monitoring

The concept of adaptive risk monitoring refers to the ability to sense or identify risk that is developing at its earliest stages so the risk can be investigated, and decisions can be made to timely eliminate or manage the risk before it adversely impacts the adviser and/or the funds. Adaptive risk is an emerging area that may become more prevalent as technology and risk frameworks evolve and use of data and algorithms become more prevalent in identifying business opportunities and emerging risks.

Historically, risk management has been based on a more reactive program. As previously discussed in the Risk events and incidents section, errors or risk events would occur, and management would perform a root-cause analysis to better understand why the event occurred and would assess the internal controls and operational practices to determine if they needed to be strengthened. Reactive risk event review and root-cause analysis should still be part of the risk monitoring framework; however, solely relying on this approach misses an opportunity to identify risks before they can result in a risk event. Sound risk management practices can be designed today so that significant risk conditions are detected at their earliest stages with rapid response.

To transition to an adaptive risk model framework, the adviser should first determine any predictable risks events that could occur and impact the funds. By thinking proactively, risk event "warning" signals can be identified, supported by an efficient process and reporting, which can alert risk managers to these conditions and allow them to begin working through the adaptive risk model to mitigate potential adverse outcomes. Consequently, efforts can then be focused on addressing the most impactful risk conditions in a timely manner while enabling an efficient use of resources.

Specific areas impacting the Investment Management industry

While an overarching risk management program can help identify and manage many risks impacting the advisers, service providers, and ultimately the funds, there are many specific risks that fund directors should consider in their oversight role. These risks fall into five categories: investment risk, technology risk, operational risk, regulatory risk, and strategic risk.

Investment risk

Director focus considerations:

- **Trend analysis:** Consider the importance of tracking investment risk trends over time, both in absolute and relative terms, to identify patterns and potential issues.
- **Performance evaluation:** Evaluate fund performance against peer groups and benchmarks on both an absolute and risk-adjusted basis to ensure alignment with investment objectives.
- **Unexpected performance:** Be prepared to investigate unexpected performance results, including significant over or underperformance, to understand underlying causes.
- **Investment process and controls:** Review the adviser's investment process and controls, including ESG risks and regulatory compliance, to ensure they support and validate the fund's strategy.
- **Risk disclosure:** Assess how a fund's risks are communicated to shareholders through disclosure documents and ensure alignment with actual risks taken.
- **Valuation risk:** Understand the implications of valuation risk, including the methodologies used for fair value determination and the potential for conflicts of interest.
- **Liquidity risk:** Ensure the fund has adequate liquidity to meet redemption requests without harming remaining shareholders, and that liquidity risk management programs are robust and compliant with regulatory requirements.
- **New product and strategy risk:** Consider the risks associated with new investment strategies and products, including the adequacy of systems, operations, and personnel to support these innovations.

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

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

- Trend levels of investment risk over time, in both absolute and relative terms
- Returns versus peer groups and benchmarks over time on both an absolute and risk-adjusted basis
- Funds with consistently weak performance
- Unexpected performance results and/or instances of significant over/under performance, and
- The adviser's investment process and controls to support and validate the funds strategy
- A fund's disclosure documents can help a board determine how a fund's risks are communicated to shareholders. Established procedures that include a comparison of a fund's actual risks (e.g., alignment with the fund's guidelines, position limits, counterparty credit limits, concentration limits, expected return volatility range) against the fund's risk disclosures can help determine whether the risks being taken are appropriate or whether the investment approach or disclosure requires adjustment.

While monitoring risk on a fund-by-fund basis is vital, such a narrow approach could expose the fund complex to added risk. For example, a risk may be relatively minor for an individual fund but could have a significant impact on the adviser's organization when aggregated, such as heightened investment risk due to exposure to a security or underlying investment across multiple funds. Therefore, in addition to discussing the fund-by-fund risk, fund directors should explore how the adviser monitors risk throughout the organization.

Considerations for fund directors

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

- Are the levels (and types) of investment risks that the adviser is taking with respect to the fund in line with a fund's prospectus and statement of additional information?
- How does the adviser measure and quantify the risks taken by the fund? Does the adviser have systems or resources in place to measure and manage those risks? What are those resources?
- Is there a qualified derivatives risk manager in place at the adviser and are there appropriate escalation protocols in place for the oversight and monitoring of risks associated with derivatives and other senior security transactions?
- How does the alpha generated by the investment compare to the risk-adjusted peer group performance?
- Is an appropriate benchmark (of similar risk profile) used for comparison of investment results?
- What types of reporting does the board receive regarding performance attribution? How often do directors receive these reports?
- How is drift within investment strategies monitored and evaluated?

Valuation risk

The 1940 Act requires funds to value their portfolio investments using the market value of their portfolio securities when market quotations are "readily available;" and, when a market quotation for a portfolio security is not readily available, by using the investment's fair value, as determined in good faith by the fund's directors.

Valuation risk is the risk that a fund inappropriately determines the value of one or more of its investments, which may result in an inaccurate net asset value for the fund. Under such circumstances, certain shareholders may be treated inequitably, bearing either more or less of the fund's returns or losses than they would otherwise. Broadly, valuation risk includes the risk that methods used for determining fair value are not appropriate (i.e., the methodologies do not provide a reliable estimate of an exit price) or have not been applied consistently or accurately.

Rule 2a-5: Good Faith Determinations of Fair Value (Rule 2a-5),[15] allows boards to designate the adviser to perform certain valuation functions (the "valuation designee"), subject to directors' oversight of valuation risks, fair value methodologies, pricing services, written fair value policies and procedures, testing of fair value methodologies, and record retention.

Among other things, Rule 2a-5 requires periodic assessment of material risks associated with the determination of fair value, including material conflicts of interest. The frequency of the reassessment of material risks is not established by the rule and may vary depending on the types of the fund's investments, significant changes in a fund's investment strategy or policies, market events, and other relevant factors. While the rule does not specify which risk(s) need to be addressed, the SEC's adopting release provides the following "non-exhaustive" list of sources or types of valuation risks:

- The types of investments held or intended to be held by the fund and the characteristics of those investments
- Potential market or sector shocks or dislocations and other types of disruptions that may affect a valuation designee's or a third party's ability to operate
- The extent to which each fair value methodology uses unobservable inputs, particularly if such inputs are provided by the valuation designee
- The proportion of the fund's investments that are fair valued as determined in good faith, and their contribution to the fund's returns
- Reliance on service providers that have more limited expertise in relevant asset classes; the use of fair value methodologies that rely on inputs from third-party service providers; and the extent to which third-party service providers rely on their own service providers (so-called "fourth party" risks)
- The risk that the methods for determining and calculating fair value are not consistent, are inappropriate, or that such methods are not applied consistently or correctly

Additional risks may be relevant, depending on the specific funds and the nature of the investments they hold, such as private equity. Refer to the "risk related to untraded investments" and "model risk" sections below for further consideration.

Considerations for fund directors

Under the framework established by Rule 2a-5, the valuation designee will provide directors with, at a minimum, quarterly and annual reporting of valuation matters, including information relevant to identified valuation risks. Directors may find the following questions helpful as they consider a fund's valuation risk and the sufficiency and frequency of valuation reporting provided by the valuation designee:

- Has the appropriate valuation designee been identified, and do they have sufficient resources to carry out their responsibilities for determining the fair value of all fund investments?

- What conflicts of interest have been identified within the valuation process and what controls have been established by the adviser to mitigate those conflicts?
- What is the role of portfolio managers and traders in the valuation process and are they excluded from voting on fair value matters?
- What are the valuation methodologies documented in the fund's valuation policies and procedures? Does the valuation designee evaluate the valuation methodologies and processes for new and evolving asset classes? For example, if a fund invests in private equity investments, what is the valuation process and how does it differ from other types of assets?
- How does the board monitor compliance with valuation policies and procedures? Has the board considered the effectiveness of controls over the valuation process?
- What constitutes a "material" valuation risk?
- Do the procedures account for changing or unusual market conditions, such as when particular markets are closed for long periods of time?
- How does the valuation designee evaluate new or current third-party pricing services, including pricing vendors, brokers, and others? How are such vendors selected for specific investments or classes of investments?
- What sort of information is provided by the fund or its advisers to third-party pricing services?
- What kind of periodic testing does the valuation designee use to test the quality of evaluated prices provided by pricing vendors?
- Does the valuation designee periodically test the secondary pricing vendor's evaluated prices?
- Do the valuation policies and procedures identify events when the board must be involved or must be notified? Are the "material" events that require board notification per Rule 2a-5 defined?
- Has the valuation designee identified key valuation indicators for each asset class that notify/inform fund directors of potential price uncertainty in the market?
- Has the board discussed with the valuation designee its expectations around Rule 2a-5's requirement for prompt notifications reporting?
- Does the valuation designee consult with pricing experts when addressing challenging or intricate fair valuation matters?
- How are issues associated with evaluating foreign securities at the close of the US stock market addressed?

Liquidity risk

Ensuring that shareholders can redeem shares in an open-end mutual fund is fundamental to a fund's operation. Rule 22e-4 requires open-end funds to develop liquidity risk management programs. The rule defines liquidity risk as "the risk that the fund could not meet requests to redeem shares issued by the fund without significant dilution of remaining investors' interests in the fund."[16] Broadly, liquidity risk includes the risk that:

- The fund does not have sufficient liquid assets or borrowing capacity, such as formal lines of credit and/or inter-fund lending facilities, to meet shareholder redemption requests in an orderly manner consistent with SEC requirements without harming remaining fund shareholders.
- Established methods to determine liquidity have not been applied consistently and/or accurately.
- Established liquidity determination methods, approaches, and/or inputs are no longer appropriate, due to changing market conditions or other factors.
- The fund's valuation procedures and policies do not appropriately consider liquidity in the valuation process to achieve accurate security valuations.
- Long-term market closures due to natural disasters, political turmoil, etc. may impact an asset's liquidity.
- The use of derivatives and other complex financial instruments may introduce additional liquidity risks, such as the potential for rapid changes in the value of derivatives positions, margin calls, or the inability to unwind positions quickly without significant market impact. In addition, the use of derivatives can introduce counterparty risk.

The rule places specific responsibilities on fund directors in their oversight of liquidity risk. Fund directors are required to:[17]

- Initially approve the fund's liquidity risk management program
- Approve the designation of the person(s) designated to administer the liquidity risk management program
- Receive and review a report at least annually regarding the liquidity risk management program, which should include notice of any material changes in the program
- Approve any changes to the fund's highly liquid investment minimum if the fund seeks to change the minimum when already below the established minimum, and
- Be informed within one business day if the fund's illiquid investments exceed 15% of the fund's portfolio.

Liquidity and valuation are closely intertwined. An asset is illiquid if the fund reasonably expects it cannot be sold in current market conditions within seven calendar days without significant changes to the market value of the investment. Further, illiquid assets frequently have to be fair valued because they do not have a readily available market quotation. Thus, there can be a direct link between the valuation of the asset and its liquidity status. Fund directors should

be aware of the possibility that selling illiquid securities to meet redemptions in stressed conditions may result in the fund receiving less than the determined "fair value" for such securities.

Additionally, derivatives and other complex financial instruments can pose unique liquidity challenges. These instruments may have less transparent markets, and their value can fluctuate rapidly, potentially leading to significant liquidity demands. A fund's liquidity risk management program should adequately address the risks associated with derivatives, including the potential for margin calls and the difficulty of unwinding positions in stressed market conditions.

Considerations for fund directors

Directors may want to consider the following questions while discussing liquidity risk with advisers:

- Does the adviser have a system to identify when funds are at risk of exceeding the established liquidity threshold?
- Does the adviser keep the board apprised of changes to the fund's liquidity risk management program?
- Is the adviser's report regarding the liquidity risk management program comprehensive?
- Does the adviser have protocols in place to notify the board, within one business day, if the fund's illiquid investments exceed 15% of the fund's net assets?

New product and investment strategy risk

Advisers continue to launch new investment strategies, structures, and vehicles, expanding into alternative investment funds, direct indexing offerings, factor-based products, and others. The types and degree of risk and the oversight practices required to manage these risks will necessarily vary, across all the categories of risk, depending on the fund strategy, structure, investment portfolio, fund size, and ongoing supporting processes.

Considerations for fund directors

Directors may consider the following relating to the risk associated with new products and/or investment strategies:

- What risks do the fund's new strategies and/or new complex investment vehicles pose beyond those identified for existing products?
- How does the adviser evaluate the appropriateness of a new fund, and the risks associated with it? For example, does the adviser have a product governance committee?
- What systems, operations, personnel/skills/talent, and technology support will the new strategy or new investment require? Do existing operations and systems require enhancement to support the new strategy or investment effectively? Do third-party service providers, such as a fund administrator, pricing vendor, transfer agent, custodian, etc. have the requisite expertise, staffing, and systems to support the new product or investment strategy?
- If the fund is sub-advised, does the adviser have adequate access and transparency into the sub-adviser to perform appropriate oversight? Is the sub-adviser experienced in managing the strategy within the confines of a fund regulated under the 1940 Act, a separately managed account, or other institutional account?
- Is the new product or strategy appropriate for the fund structure? For example, would the product or strategy be more suitable for a closed-end fund or vehicle with less daily liquidity needs?
- Is the adviser able to execute the new strategy while also adhering to any existing limitations (e.g., leverage, liquidity), whether due to regulatory restrictions or policy/strategy restrictions? Are these products periodically stress tested under various historical and hypothetical scenarios?
- Do existing valuation policies, procedures, and controls address valuation risks associated with new products or strategies?
- Have additional risks specific to new products and strategies been appropriately disclosed to investors in the prospectus, fund marketing materials, and other fund offering documents?
- Has a time frame been established with goals for measuring the success of a new product?
- How will the fund board reporting need to be updated to provide appropriate oversight of these new risks?

Alternative, untraded investment risk

Alternative, untraded securities, such as private equity ("alternative investments"), may offer advisers the ability to earn additional alpha and diversify investment risk from public equities. As a result, registered funds are increasing their holdings in alternative investments as evidenced by the Deloitte Fair Valuation Pricing Survey 22nd Edition.[18]

Private markets require stronger emphasis on due diligence and valuation considerations. These investments have several unique structural features including lack of liquidity, reliance on fair valuation instead of mark-to-market valuation, quarterly performance reporting, uncertainty about the timing of capital deployment, and a reduced transparency into the underlying holdings. As such, funds allocating investment dollars to alternative investments present several additional factors for their directors to consider, including:

- Is the investment objective of the fund compatible with an allocation, given the unique nature of private markets?
- What are the policies and controls surrounding allocations to alternative investments?
- How does the adviser assess the risk levels associated with alternative, non-traded ("alternative") investments? Does the adviser have the right skills to account for, report, and value such alternative investments?

- Does the adviser have a rightsized and properly resourced due diligence team to analyze the investments?
- How will the adviser assess potential conflicts of interest given the reduced transparency related to underlying holdings?
- How are the holdings fair valued?
- Are the appropriate valuation policies and procedures in place that incorporate the methodologies around valuation of the alternative investments?
- Does the adviser have an internal valuation team able to value the investments and will the outside auditors be able to independently evaluate the valuations?
- What monitoring and review policies are in place for each alternative investment?
- What frequency of valuation will be performed?
- Based on significant events (i.e., microeconomic, industry, company specific), what is the process to update valuations on an inter-period basis (i.e., once a significant event has occurred, how quickly will a revised valuation be performed? What factors are considered? Who will perform the valuation?)?
- What is the adviser's ability to monitor for conflicts of interest in alternative investments?

Albeit less prevalent than initially anticipated, private companies have utilized special-purpose acquisition companies (SPACs) as a means of accelerating their ability to go public via an initial public offering (IPO).

A SPAC is a publicly traded company that uses a combination of IPO proceeds and additional financing to fund the acquisition of a private company (known as the "target company"). Deal announcement to deal closing dates vary widely but can be as short as four to six months. This accelerated timeline has been instrumental in the growing number of companies going public through SPAC transactions.

Considerations for fund directors

Directors may find the following questions helpful as they perform oversight over the adviser's decisions to invest in SPACs:

- Has the adviser performed due diligence regarding the SPAC?
- Has the adviser considered risks unique to the SPAC structure?
- Is an investment in SPACs consistent with the fund's investment objectives?
- Has the SPAC been able to execute on acquisition of a target company in the allotted time frame?
- Are there particular valuation concerns about acquiring pre-IPO securities through a SPAC rather than directly through a private placement?

Environment, social, and governance (ESG) risk

Investing according to ESG principles continues to garner attention from investors, the public, and regulators. Advisers who wish to incorporate ESG factors into their investment processes face many considerations as they move forward, including:

- The lack of an agreed-upon US regulatory definition of what constitutes ESG
- An evolving market and regulatory ESG landscape both inside and outside the United States
- Appropriate market or company proprietary data to support ESG investments and reporting can be difficult to obtain, and investment decisions may also include qualitative factors that make comparisons among potential investments difficult
- Advisers engaging sub-advisers have the additional complexities of understanding the ESG approach utilized by each sub-adviser, and
- Demonstrating conclusively that the adviser is managing the funds in accordance with its ESG guidelines and disclosure documents.

Over the last few years, regulatory bodies have increasingly targeted fund companies for ESG-related violations, particularly focusing on misleading claims or failures to adhere to ESG investment policies, often culminating in multimillion-dollar fines and reputational damage. Common infractions include the absence of written ESG policies, inconsistent adherence to such policies when they do exist, misstating claims that funds incorporate ESG factors, and inaccurately marketing funds as integrating ESG criteria. These discrepancies between ESG marketing and actual investment processes have drawn significant scrutiny and enforcement actions.

Considerations for fund directors

Directors overseeing ESG funds may wish to understand:

- How does the adviser approach its use of ESG—as a hedge against potential investment risk or as an investment philosophy?
- How is the fund's ESG process described in disclosure documents? Is the investment process used by the fund consistent with that description?
- How is compliance with disclosure tested?
- How does the adviser consider the impact of state and federal regulatory scrutiny of ESG investments?

Technology risk

Director focus considerations:

- **IT infrastructure and security:** Understand the current state and suitability of the technology infrastructure, including the security measures in place to protect sensitive data and transactions.
- **Cloud migration strategy:** Assess the adviser's strategy for migrating to cloud service providers, including the alignment with organizational goals and the management of incremental cloud security risks.
- **Governance and controls:** Evaluate the governance and control mechanisms in place to prevent IT failures, unauthorized transactions, and data breaches.
- **Cybersecurity strategy:** Review the adviser's risk-based cybersecurity strategy, including the alignment with business and IT strategies, and the resources allocated to manage IT/cyber risk.
- **Incident response and resiliency:** Understand the preparations and plans in place to respond to ransomware attacks, data breaches, or other cyber incidents, including the existence of an incident response plan.
- **Model risk management:** Evaluate the adviser's approach to managing model risk, including the validation of model outputs, change management procedures, and independent validation of models.
- **Artificial intelligence risks:** Assess the adviser's use of AI, including the monitoring of AI usage, data used for training models, and the mitigation of biases and data breaches.
- **Vendor management:** Review the due diligence, monitoring, and management of outsourced IT services, including the definition of responsibilities and legal liabilities during incidents and investigations.

Information technology (IT) risk

Technology enables virtually every activity or service that an adviser and the funds' other service providers undertake or deliver. The reliability and the security of technology is critical to providing those essential services and ensuring sensitive data and transactions are secure. For example, the rising trend in migrating to cloud service providers (CSPs) from traditional on-premises infrastructure has increased the importance of appropriate visibility, governance, cloud security and identity, and access management controls (see below). Weak governance and controls can lead to failed IT investments, system failures, processing errors, unauthorized transactions, and data/compliance breaches. Further, regulators continue to focus on the safety and soundness of data and technology in addition to compliance with laws and regulations.

Industry-leading CSPs offer organizations new business and valuable IT capabilities. Organizations have increased their adoption of cloud technologies for reasons such as lower costs, integrated security, scalability, flexibility, functionality, including generative AI, and availability of intelligent analytics. Advisers should proactively implement cloud security controls and institute risk assessment and mitigation plans to realize the benefits of cloud and other enabling technologies safely. The effective management and governance of IT risk depends on both the senior executive team— including, as applicable, the chief technology officer (CTO), CRO, and chief information security officer (CISO)—as well as a broad set of accountable managers from across the organization. While IT risk management frameworks vary from organization to organization, effective IT risk management helps drive a practical and consistent operating model across all IT domains (e.g., IT strategy, data management, service delivery, and operations) to identify, manage, and address risks. Directors are not required to be IT experts to oversee technology risks, but they should inquire about the IT landscape to fulfill their oversight responsibilities.

Considerations for fund directors

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

- Is IT risk appropriately covered in the risk reporting provided to the fund board?
- What key IT initiatives are under consideration or underway that will impact the funds, and what data sets and information does the board receive on these initiatives and impacts?
- What is the relevant technology infrastructure, and the suitability/condition of the infrastructure, at the adviser and other key service providers?
- What key operations of the IT platform and structure have been outsourced?
- If the adviser or other key service providers are considering migrating infrastructure to a cloud service provider, is the cloud migration strategy and road map aligned with IT and organizational goals? Does management have appropriate resources in place to identify and manage incremental cloud security risks? Are these resources continually trained in the latest and greatest practices to drive secure cloud adoption? Has management considered enhancing current incident management capabilities and processes to scale for the evolving cloud threat landscape?
- Does the fund have proprietary applications that should be assessed from a security perspective (dynamic and static application security testing, secure code analysis, etc.)?
- Is there effective due diligence, monitoring, and vendor management over outsourced IT services? Are service provider and subscriber responsibilities clearly defined and does vendor management over IT services appropriately consider legal liability, insurance coverage, and roles during incidents and investigations?

Information (cyber) security risk

The SEC staff has consistently indicated that cybersecurity is a priority in their examinations of market participants, including advisers, as evidenced by the proposed cybersecurity rule.[19] In the SEC's assessment of how firms prepare for a cybersecurity threat, safeguard customer information, and detect potential identity theft flags, it has focused on a number of areas including governance and risk assessment, access rights and controls, data loss prevention, vendor management, incident response, and training, among others.

Key considerations for fund directors

Directors may find the following questions helpful as they consider a fund's cybersecurity risks:

- Has the adviser established a risk-based cybersecurity strategy that aligns with overall business and IT strategy?
- Have cross functional leaders defined organization-wide IT risk and cybersecurity policies, standards, and procedures that are aligned with the funds' strategic and business goals?
- Has the adviser done a cyber risk assessment to understand the overall program maturity, risk, and prioritization roadmap?
- Has the adviser identified the funds' key assets and where they exist?
- Does everyone in the organization understand the adviser's cyber risk appetite?
- Does the CISO (or equivalent) have the resources necessary to manage IT/cyber risk? What training is given to employees regarding cybersecurity?
- What preparations are in place to operate during a ransomware attack, breach, or incident? Does the adviser have an incident response plan and a strong resiliency program?
- Does the adviser have cybersecurity insurance?
- When would the board be notified regarding a data breach and/or cyber incident?

Data risk

Ineffective data management can lead to issues including business disruption and loss, fund financial and regulatory reporting issues, privacy issues, and/or loss of investors' trust. Regulatory agencies are also becoming more data savvy and continue to actively monitor data, given that advisers depend on accurate, complete, and timely data. Funds can manage core data risks such as data quality risk and data privacy risk, while also identifying and mitigating emerging data risks, such as unstructured data risk, third-party risk, and emerging technology risks (e.g., application of AI/machine learning (ML)). A structured approach to data risk management may help organizations in enhancing the accuracy, completeness, and timeliness of data, and in maintaining clear data accountability, and appropriate data use. Identification of data risks across the data lifecycle (i.e., controlled capture, transformation, use, and archival/disposal of data) could serve as a starting point for funds on their data risk management.

Considerations for fund directors:

Directors may find the following questions helpful as they consider a fund's data risks:

- Have data-related policies and standards for data risk identification, mitigation, and accountability been defined and established?
- Has a data governance model been constructed?
- Are the three lines of defense (i.e., front line operations, risk and compliance management, and internal audit) working in tandem to holistically identify and manage data risks?
- How are data risks defined, aggregated, reported, and monitored by the board and other management stakeholders?
- Are investments in technology solutions/platforms aligned to the fund's goals of minimizing data risks?

Model risk

With the increased reliance on technology to enhance and standardize the investment processes, more funds rely on models. Advisers use models for asset selection, risk management, allocation of positions between funds, and other operational functions. This includes rules-based and smart beta products, such as proprietary indexes, which are designed to systematically capture specific investment factors or market inefficiencies. Model risk is the potential risk for adverse consequences from decisions based on incorrect or misunderstood model outputs and reports. Model issues can lead to monetary loss, harm to clients, erroneous financial statements, improper investment or managerial decisions, and/or damaged reputation resulting from poorly constructed, interpreted, and maintained models. Given the complexity and reliance on these sophisticated models, it is crucial to highlight and consider the inherent model risk associated to ensure robust and reliable outcomes.

Model issues have occurred where:

- New models or model updates/changes are not appropriately developed, tested, or validated
- Model elements (e.g., algorithmic formulas) are not properly maintained and updated when new data becomes available
- Modification to existing model algorithm and/or data is not identified, well managed, or understood by those relying on the model
- Model assumptions are not tested adequately resulting in faulty results, and
- Models or model changes are not fully understood by those relying upon them.

Regardless of the cause, model issues and failures may be very costly to identify, investigate, and remediate—potentially causing significant erosion in value, including reputational loss, regulatory sanctions, and economic and financial losses.

Considerations for fund directors

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

- How does the adviser define models?
- How does the adviser manage model risk? Does the adviser have a robust model risk management program?
- How are model outputs validated?
- What is the difference between models that make automated investment transactions and tools used as inputs in the portfolio manager's decision process?
- Who in the organization oversees model risk, and do they have the ability and authority to effectively challenge model owners? Are models subject to independent validation prior to being put into production?
- Who reviews model recommendations prior to implementation?
- Does the adviser have a process for how model inputs can be changed?
- Are there post-implementation and annual model risk reviews?
- How does the adviser review and test third-party or vendor models?
- How often is back testing conducted on rule based and smart beta products?
- Have appropriate peers been identified for benchmarking?
- What type of regular reporting does the board receive on significant model risks, both for specific models and in the aggregate?
- Does the adviser have change management procedures and controls in place to appropriately capture and record model changes over time?
- What defines an error or incident?
- Does internal audit or a third party perform a periodic audit to determine that model risk activities, framework, and model outputs/valuations are being performed adequately based on policy?

Artificial intelligence (AI) risk—New in 2025****

Artificial intelligence's powerful analytics and ease of use are transforming many business sectors, including the investment management sector. The use of artificial intelligence in financial services, such as for decision-making, client communications, and model generation, poses unique risks like market manipulation, ethical concerns, and intellectual property issues. Investment managers must thoroughly assess these emerging risks.

Considerations for fund directors

Directors may find the following considerations helpful as they consider IT risk:

- Does the board understand how AI is deployed and utilized by the adviser? How is AI use monitored by the adviser?
- Does an inventory or catalog from the adviser and affiliated service providers exist, detailing AI usage and risk assessment categorization (e.g., high, medium, or low)?
- What data is being used to train the artificial intelligence models? Advisers must ensure that data used for training complies with privacy laws. Sensitive client or proprietary data must be anonymized or protected.
- How are data breaches being mitigated? Cybersecurity protocols must be robust enough to prevent unauthorized access to models or data.
- How does the adviser assess and monitor model fairness? Regular audits should be conducted to ensure AI outputs are equitable across demographics.
- Can the adviser explain how the artificial intelligence model reaches its conclusions? AI models should be able to be explained in plain English to enable effective compliance and oversight, particularly for decisions that affect clients or regulatory filings.
- What level of transparency does the third-party provider and/or adviser offer regarding AI decision-making? The board may inquire about key elements of the AI's decision logic to manage potential risks effectively.
- Is there a robust process for testing and validating artificial intelligence models? Models should undergo rigorous testing, including stress tests, back-testing, and scenario analysis, to ensure they perform as expected in different market conditions. Independent validation of AI models can reduce risks of internal bias or oversight, ensuring that models function properly before they are deployed.
- How does the adviser balance human oversight with artificial intelligence usage? While AI can automate decision-making, overreliance without human oversight can increase operational risk, especially in complex or unforeseen situations.
- Are there processes in place to ensure human accountability for AI outputs? Accountability frameworks should ensure that AI-driven decisions have human sign-off, especially in high-stakes decisions.
- Are model changes and updates thoroughly tested before implementation? Any updates to artificial intelligence models should be carefully reviewed and validated to prevent unintended consequences.

- Is there transparency with clients/investors regarding the use of AI? Investors may need to be informed about when AI is being used to provide recommendations or manage portfolios, especially if AI influences investment outcomes.
- Who is responsible if artificial intelligence makes an erroneous or harmful decision? Directors may wish to define clear accountability in case AI decisions lead to significant financial or reputational damage.
- What contingency plans are in place if AI systems fail? Disaster recovery and alternative strategies should be in place to manage failures in AI systems.
- Is the use of artificial intelligence overseen by a governance committee within the organization?

Operational risk

Director focus considerations:

- **Regulatory compliance:** Ensure that day-to-day operations adhere to relevant regulatory requirements and guidelines to avoid legal and compliance issues.
- **Incident management and recovery plans:** Understand the existence and adequacy of recovery plans and incident management protocols to respond to operational disruptions.
- **Conflict of interest management:** Identify and manage conflicts of interest, particularly in smaller firms, to maintain operational integrity and trust.
- **Operational monitoring and assessment:** Review how operational processes are monitored and assessed to identify areas for improvement and ensure continuous enhancement.
- **Tax risk management:** Ensure that tax risks are adequately managed, and regular tax testing is conducted to optimize tax outcomes, especially for new and smaller funds.
- **Business resilience:** Evaluate the adviser's business continuity and IT disaster recovery plans, including the consideration of climate risk and the ability to respond to severe disruption scenarios.
- **Third-party risk management:** Understand how the adviser manages third-party provider risks, including the use of continuous monitoring techniques and AI-based tools to enhance oversight.

Day-to-day operations—**New in 2025**

Fund operations are inherently complex and multifaceted, necessitating seamless coordination across various functions to ensure the fund meets its investment objectives, complies with regulatory requirements, and provides exceptional service to investors. Effective operations are paramount to maintaining investor trust and achieving long-term success. Key operational areas include regulatory compliance, accurate financial operations, effective portfolio management, robust administration, excellent investor services, strategic sales and marketing, reliable technology infrastructure, strong governance, and diligent tax management.

Errors or incidents in the day-to-day operations of a fund can have significant and wide-ranging consequences, such as financial losses, reputational damage, operational disruptions, legal and compliance issues, tax penalties, and negative impacts on clients and stakeholders. Therefore, advisers and key service providers should have robust systems, controls, and processes to minimize the risk of errors and effectively manage any incidents that may occur.

Directors play a critical oversight role, focusing on core operations while maintaining a clear distinction between oversight and day-to-day management. Directors should work closely with counsel to understand these boundaries and avoid stepping into management roles. Directors should work closely with management to understand the operational risks involved in the business and how such risks are mitigated.

Additionally, conflicts of interest, particularly in firms with inadequate segregation of duties, are a key focus for regulators. Therefore, directors must remain vigilant in identifying and mitigating conflicts of interest to uphold the integrity and trustworthiness of the fund.

Considerations for fund directors

Directors may find the following questions helpful as they consider a fund's day-to-day operations:

- Do operations adhere to relevant regulatory requirements and guidelines?
- Are robust systems, controls, and processes in place to minimize the risk of errors?
- Do recovery plans and incident management protocols exist to enable a suitable response when events occur?
- Is there a clear distinction between director oversight and day-to-day management?
- How are conflicts of interest identified and managed to prevent conflicts from affecting operational integrity?

- Are the appropriate governance frameworks in place to ensure accountability?
- How are operational processes monitored and assessed to identify areas for improvement?
- Are tax risks adequately managed, and is regular tax testing conducted to ensure compliance and optimize tax outcomes?

Business resilience

Business continuity (BC) and IT disaster recovery (DR) are concepts that have been implemented at corporations for several decades. The threat landscape, dependence on technology and client service expectation of the 2020s have prompted organizations to identify and analyze the severe, but plausible, disruption scenarios that could impact their business services. In addition, the emergence of climate risk has added another threat to the landscape that advisers may need to address. Regulators are also becoming much more active in rule making and guidance on a global scale (OFSI, B-10, Bank of Ireland Business Resiliency guidance, and the SEC proposed rules on cybersecurity). This information may be helpful for reference and in assessing readiness of the fund organization in the event of a disruption. They have transformed the traditional BC and DR concepts and designed a new operational resilience framework that enables organizations to respond swiftly to outages, disruptions, and crisis events in a coordinated and holistic manner.

These six steps can serve as a guide for firms to help achieve operational resilience:

- Understand the disruption scenarios that could cause client impact and provide actionable intelligence to key decision-makers
- Develop strategies and scenario playbooks, and test regularly through risk scenario table-top or similar exercises that can be used to respond and recover from those situations
- Focus on the critical end-to-end business (aka "heartbeat") services that are client facing and implement aggressive recovery times
- Aggregate "resilience data" that enables the organization to respond with the best possible information.
- Validate and measure the demonstrated resilience capabilities through rigorous simulations and technology testing
- Maintain a backup plan for key service providers if they experience a significant or prolonged outage (e.g., a backup pricing vendor).

This operational resilience framework helps organizations focus their investment and effort on those things that impact clients, regulators, and the overall financial system. Those organizations that implement operational resilience concepts will have a higher degree of confidence that the critical business functions can be recovered following a significant disruption.

Considerations for fund directors

When discussing how advisers and service providers manage resiliency, directors may want to consider:

- What recovery plans does the adviser or service provider have in place?
- What evidence exists to demonstrate that the adviser can respond and recover the end-to-end business service within the expected time frames? Does the adviser have insights into the infrastructure, third party and applications that the business services depend upon for efficient decisions?
- Do the relevant parties within the adviser have a clear understanding of their responsibilities? Do directors and executives understand how they will be involved and make decisions during a crisis event or disruption? Do the recovery team members have a clear understanding of their roles and responsibilities? Has the adviser simulated those? What happens if a critical third party is impacted by an extended disruption?
- Has climate risk been considered and evaluated as part of the recovery plans?
- How and how often are the strategies and playbooks tested? Are the tests designed to identify potential gaps?

Third-party provider risk

The fund industry continues to increase its reliance on third-party organizations such as vendors and service providers to perform a variety of critical activities, including those performed by advisers/sub-advisers, fund administrators, custodians and accounting agents, transfer agents, pricing vendors, and sub-accounting organizations, as well as internal service providers (e.g., affiliates).

Third-party service providers play a major role in the growth of advisers, as organizations have come to rely on service providers to handle many core business activities, and while each of those presents opportunities including cost savings and improved efficiencies, there are potential risks that need to be identified and managed in a structured manner.

Third-party risk management (TPRM) as an organizational discipline has evolved from a fragmented approach with different parts of the organization (i.e., compliance, IT) managing third-party risk in silos, towards a structured governance-driven programmatic approach to overseeing an ecosystem of third parties, and it has proved to be essential. The SEC continues to emphasize the importance of adequate third-party oversight through its examination priorities and guidance on business resiliency connected to the use of third parties as well as through its priority focus areas during examinations in areas such as third-party cybersecurity.

Moving toward next-gen TPRM

While traditional TPRM activities such as vendor questionnaires and review of SOC1/SOC2 reports are still recommended, organizations may continue to move towards continuous monitoring techniques for critical service providers to move away from solely relying on point-in-time assessments. Emerging key risk data providers such as those who can communicate near-time information on cybersecurity, negative news, and financial risks to name a few, now play a key role in helping organizations compile and analyze risk information, generating a transparent, constantly updated view on risks. This also facilitates point-in-time assessments to be more effective as a risk-based/focused approach can be taken when correlating the continuous monitoring efforts.

TPRM programs are evolving in several other ways, including:

- Using AI-based monitoring of third-party service providers and synthesis of information for executives' organization-wide, to improve transparency and challenge the traditional, more costly methods of oversight
- Helping leaders see and counter vulnerabilities as they materialize in real-time
- Turning third-party risk into opportunity, and
- The development of system applications to enable the effective and efficient oversight of TPRM activities.

Considerations for fund directors

When discussing third-party risk management, directors may want to consider:

- How does the adviser think about its third-party risk management? How does it see the program evolving?
- Has the adviser conducted a third-party inventory that is widely available in the organization?
- How does the adviser assess its critical service providers? For example, has the adviser established a tiered approach to third-party risk management that identifies the most-critical services providers and vendors and manages the risk presented by those entities accordingly?
- How is the adviser using technology to enhance its monitoring of service providers?
- How often does the adviser review its program to identify areas of enhancement?

Regulatory risk

Director focus considerations:

- **Monitoring regulatory changes:** Understand how the adviser monitors evolving regulatory issues and ensures compliance with new and existing regulations.
- **Board reporting:** Assess the quality and comprehensiveness of the information provided to the board regarding the implementation of new regulatory requirements and compliance trends.
- **Due diligence on sub-advisers:** Ensure that the adviser conducts thorough due diligence and monitoring of sub-advisers for regulatory compliance.
- **AML program effectiveness:** Evaluate the effectiveness of the fund's AML program, including policies, procedures, training, and independent testing.
- **Third-party oversight:** Understand the oversight mechanisms for third-party service providers involved in the AML program and other regulatory compliance areas.

Regulatory compliance risk

Regulatory compliance risk includes the risk that the fund, the fund's adviser, and other key service providers fail to comply with existing regulatory requirements and the follow-up associated risks of fines, litigation costs, reputational risk, or enforcement actions by regulators as well as the risk of failing to identify and timely implement new or evolving regulations.

The current regulatory environment is dynamic and increasingly complex. In addition to regulations from the SEC, other regulations may have a profound impact on the fund industry as well. For example, US banking regulators, such as the Federal Reserve and Office of the Comptroller of the Currency, are increasingly exerting their influence over bank holding company/bank-owned advisers. Further, the increasingly global footprint of the industry has also added to the complexity of overseeing regulatory risk management efforts, as foreign regulatory or legislative actions may impact the operations of US funds or their advisers.

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

Considerations for fund directors

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

- How are regulatory issues monitored and by whom?
- What information is provided to the board regarding the implementation of new regulatory requirements?
- Who ensures the adviser ensure existing laws and regulations are followed?
- How does the adviser track enforcement and regulatory actions by regulators other than the SEC, as applicable?
- What reporting do the fund directors receive to understand regulatory compliance trends and the risks that they may pose?
- How does the adviser's due diligence regarding sub-advisers monitor for regulatory compliance?

Disclosure risk

The 1933 Act requires, among other things, that a majority of the board sign a fund's registration statement prior to filing, imposing liability for any material misstatements or omissions. Thus, directors need to be aware of the risk that fund disclosures could contain an untrue statement of a material fact or omit a material fact required to be stated or necessary to make the statements contained therein not misleading. The board should understand the processes and responsibilities of all parties involved in preparing and updating fund disclosures.

In addition to financial risk, the SEC has pursued enforcement actions against fund groups for disclosures that have failed to properly inform shareholders of potential risks. In certain cases, these actions were based on a lack of disclosure regarding how a fund's returns would change as the fund grew due to the impact of IPOs and pricing policies.

Considerations for fund directors

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

- Do the adviser, fund counsel, and others relied upon by the board have sufficient controls to determine that disclosures and statements included in fund documents are are appropriate and remain current?
- Do the adviser, fund counsel, and others relied upon by the board have appropriate controls to identify appropriate disclosures or risks as the funds engage in new investment types?

Money laundering risk

Money laundering is the act of disguising the proceeds of illegal activities through a series of financial transactions to make it appear as if they originated from legitimate sources; in this way, "dirty money" is "cleaned." With increased regulatory pressure on the banking industry and substantial dollars flowing to and from money laundering and terrorist organizations, there is a risk that funds may be viewed as an alternative place for money launderers to place their illicit dollars. The increased prevalence of digital assets and cryptocurrency and their attractiveness to criminals as a means to place their illicit dollars, adds further complexity to funds' anti-money laundering (AML) programs for those funds with exposure to these areas.

Mutual funds are required to have an AML program that includes, among other requirements:

- Board-approved policies, procedures, and internal controls reasonably designed to prevent the fund from being used for money laundering or the financing of terrorist activities
- Designation of a person (the "AML officer") responsible for implementing and monitoring the operations and internal controls of the AML program
- Ongoing anti-money laundering training of fund personnel
- Implementing customer identification programs including understanding and collecting beneficial ownership for legal entity customers
- Conducting ongoing customer due diligence to understand the nature and purpose of customer relationships and to develop a customer risk profile
- Processes for enhanced due diligence for certain high-risk customers (e.g., foreign correspondent accounts)
- Monitoring, identifying, and timely reporting of suspicious activity
- Various reporting and recordkeeping requirements and information sharing with law enforcement and financial institutions, and
- Independent testing of the AML program by independent fund personnel or a qualified third party.

Considerations for fund directors

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

- Does the fund have a process to regularly review regulatory requirements, regulatory guidance, and recent AML enforcement actions to determine whether a fund's AML program, or its policies and procedures, should be changed or enhanced?
- Does the fund delegate aspects of its AML program to a third party (e.g., a transfer agent), and if so, does it have the appropriate oversight and metrics to demonstrate effective governance of the AML program as well as third parties that support it? Is initial and ongoing due diligence performed on the third party?
- Has the fund's administrator, transfer agent, or custodial bank been subject to an enforcement action? If so, what, if any, effect did the enforcement action have on the fund's investors?
- Is annual independent testing of the fund's AML program conducted? If so, what deficiencies or enhancement opportunities were identified in recent reports and have management action plans been developed to address them?

Strategic risk

Director focus considerations:

- **Reputation management:** Evaluate the adviser's efforts to define and build its desired reputation with key stakeholder groups and monitor reputational risks.
- **Crisis preparedness:** Assess the adviser's crisis response plans, including periodic testing and improvement of these plans to ensure readiness for reputational events
- **Proactive trust building:** Review the proactive steps taken by the adviser to build trust and strengthen its brand and reputation.
- **Human capital strategy:** Consider the firm's strategies for attracting, retaining, and upskilling talent in a competitive market, including the adoption of flexible work arrangements.
- **Digital transformation:** Evaluate how the firm leverages digital tools, technologies, and AI to enhance productivity, decision-making, and customer experiences.
- **Continuous learning and innovation:** Assess the firm's commitment to fostering a culture of continuous learning, development, and innovation, including investments in research and development.

Reputational risk and crisis management

Reputational risk can be viewed as a loss of trust in or increase in negative perception of the fund or the adviser that can lead to negative publicity, fund redemptions, and loss of future fund investments with follow-up on impacts to the fund's operations as a result. With advancements in social media and Generative AI (GenAI), the speed at which information spreads digitally has exponentially increased, including the rapid dissemination of misinformation. This creates additional reputational challenges for organizations to navigate. As such, reputational risk should be proactively managed. Many advisers now have formal programs that focus on reputation management and are well prepared to respond to reputation-damaging or crisis situations. Targeted efforts to build and create the desired reputation are crucial, as a strong reputation is an asset that can wield significant influence in the market. By building up a robust reputation, advisers can ensure that clients are more likely to remain loyal and supportive during a crisis event. Additionally, when the fund complex is only one of the adviser's lines of business, issues in another part of the business may impact the funds. Therefore, fund directors should appreciate how the fund fits within the adviser's overall business and the risks to the funds associated with these additional business lines.

Considerations for fund directors

Directors may wish to consider the following relating to reputational risk and crisis management:

- How are risks, risk events, or actions that may cause reputational damage identified and monitored? Does the adviser perform reputational risk sensing or intelligence gathering activities?
- Is the adviser crisis-ready and well prepared to navigate a reputational event? Are crisis response plans periodically tested and improved upon?
- How is the fund board engaged and informed of potential reputational risk events and crisis mitigation strategies?

Human capital risk—**New in 2025**

Recent workforce changes, driven by evolving employee expectations, flexibility needs, and rapid technological advancements, have necessitated a shift in talent strategies towards hybrid and remote work models. This shift, coupled with the increasing complexity of products and services, is making it more challenging for firms to find and retain a talented workforce. Consequently, firms are focused on identifying external talent and training internal staff to build bench depth and upskill the current workforce. The transition to hybrid working models may support greater work-life balance and allow funds, advisers, and service providers the ability to tap into a global talent pool and enhance capabilities. Embracing digital transformations, such as automation, data analytics, and cloud computing, has become essential to streamlining operations and boosting productivity. The integration of AI also enables data-driven decisions, personalized investor experiences, and the ability to improve overall efficiency. Therefore, obtaining, retaining, and upskilling talent introduces significant risk to be able to keep pace with an ever-changing landscape. To maintain a competitive edge, advisers and service providers should focus on fostering innovation and equipping their workforce with advanced tools, continuous training, and robust cybersecurity tools. Failing to adapt to these changes could result in talent attrition, operational inefficiencies, and falling behind competitors.

Considerations for fund directors:

Directors may wish to consider the following relating to human capital risk:

- How does the firm plan to attract top talent in a competitive market?
- What measures are the firm taking to retain top performers?
- Is the firm offering flexible work arrangements that meet the needs of its employees?
- How is the firm fostering a positive and inclusive workplace culture?
- Is the firm leveraging the latest digital tools and technologies to enhance productivity?
- How is the firm utilizing AI to improve decision-making and customer experiences?
- What investments are being made in research and development to drive innovation?
- How is the firm encouraging a culture of continuous learning and development?
- Does succession planning exist for key roles?

Conclusion

The oversight of risk is a key component of the general oversight responsibilities of registered fund directors. Risk is inherent in the investment management industry and the decision of which risks to undertake and how to monitor or mitigate them is critical for the success of the adviser as well as a fund and its shareholders. While not responsible for risk identification, analysis, and management, fund directors may play a critical role in effective risk governance. This MFDF Risk Management White Paper is designed to help fund directors enhance their knowledge of risk management frameworks and many of the investment, technological, operational, and strategic risks that registered funds face in a rapidly changing regulatory environment.

Mutual Fund Directors Forum Risk Management Oversight Working Group

Stephanie Brown
Chief Compliance Officer
Fidelity Investments

Donald Burke
Trustee
Virtus Funds

Chris Cheeseman
Director
American Century

Robert J. Chersi
Director
Thrivent Funds

Anne Choe
Partner
Simpson Thacher & Bartlett LLP

Dianne Descoteaux
Senior Counsel
Mutual Fund Directors Forum

Paul Diouri
Head of Americas Risk
Invesco

Karl Ehrsam
Principal and Investment Management Risk & Financial Advisory Leader
Deloitte & Touche LLP

John Kelly
Independent Trustee
Victory Capital

Paul Kraft
Partner and Investment Management Marketplace Excellence Leader
Deloitte & Touche LLP

Padel Lattimer
Independent Director
Principal Funds

Kim Patmore
Independent Trustee
Charles Schwab

Amy Shelton
Chief Compliance Officer
American Century

Charles Rizzo
Adjunct Professor
Operations and Risk Management
Bentley University

Robert Gartland
Director
Fidelity Investments

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

Alex Bierman, Manager, Deloitte & Touche LLP
Alex Brady, Principal, Deloitte & Touche LLP
Keri Calagna, Principal, Deloitte & Touche LLP
Lauren Campson, Senior Manager, Deloitte & Touche LLP
Sarah Digirolamo, Partner, Deloitte & Touche LLP
Rich Doyle, Senior Manager, Deloitte & Touche LLP
Janice Durisin, Managing Director, Deloitte & Touche LLP
Anca Ferent, Senior Manager, Deloitte & Touche LLP
Craig Friedman, Managing Director, Deloitte & Touche LLP
Paul Gasaatura, Senior Consultant, Deloitte & Touche LLP
Maria Gattuso, Principal, Deloitte & Touche LLP
Clifford Goss, Partner, Deloitte & Touche LLP
David Guthrie, Manager, Deloitte & Touche LLP
Joshua Hanna, Principal, Deloitte Transactions and Business Analytics LLP
Sunil Kapur, Managing Director, Deloitte & Touche LLP
Tiffany Kleeman, Managing Director, Deloitte & Touche LLP
Zack Martin, Manager, Deloitte & Touche LLP
Bryan Morris, Partner, Deloitte & Touche LLP
Justin Panicker, Senior Manager, Deloitte & Touche LLP
George Psarianos, Managing Director, Deloitte & Touche LLP
Asma Qureshi, Senior Manager, Deloitte & Touche LLP
Jonathan Rizzo, Principal, Deloitte & Touche LLP
Michael Segala, Principal, Deloitte Consulting LLP
Anish Srivastava, Managing Director, Deloitte & Touche LLP
Alexey Surkov, Partner, Deloitte & Touche LLP
Bruce Treff, Managing Director, Deloitte & Touche LLP
Snehal Waghulde, Managing Director, Deloitte Consulting LLP
Damian Walch, Managing Director, Deloitte & Touche LLP
Craig Wiebman, Partner, Deloitte & Touche LLP

Endnotes

1. Role of the Mutual Fund Director in the Oversight of the Risk Management Function May 2022

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

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

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

5. See, e.g., Section 15(c) of the 1940 Act: Section 2(a)(41) of the 1940 Act.

6. The SEC has explicitly stated, "directors play a critical role in policing the potential conflicts of interest between a fund and its investment adviser" and the SEC has indicated that "[t]o be truly effective, a fund board must be an independent force in fund affairs rather than a passive affiliate of management." Interpretive Matters Concerning Independent Directors of Investment Companies, 1940 Act Release No. 24083 at 3 (Oct. 14, 1999) ("Interpretive Matters Adopting Release"); Investment Company Governance, 1940 Act Release No. 26520 at 3 (July 27, 2004) ("Fund Governance Adopting Release").

7. See, e.g., Rule 38a-1 under the 1940 Act, which requires a fund's board to approve the policies and procedures of the fund's investment advisers, underwriter, administrator, and transfer agent. See also Interpretive Matters Adopting Release. ("The [1940] Act requires that a majority of a fund's independent directors: approve the fund's contracts with its investment adviser and principal underwriter; select the independent public accountant of the fund; and select and nominate individuals to fill independent director vacancies resulting from the assignment of an advisory contract. In addition, rules promulgated under the [1940] Act require independent directors to: approve distribution fees paid under rule 12b-1 under the [1940] Act; approve and oversee affiliated securities transactions; set the amount of the fund's fidelity bond and determine if participation in joint insurance contracts is in the best interest of the fund.")

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

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

10. See Proxy Disclosure Enhancements, SEC Release No. 33-9089; 34-61175; IC-29092; File No. S7-13-09 (December 16, 2009) at 43–44. The release adopted rules requiring funds to describe the board's role in risk oversight. In that release, the Commission acknowledged that "risk oversight" was a more appropriate way to describe the board's responsibilities for risk than "risk management." The Commission stated that the disclosure could provide important information about how a fund perceives the role of its board and the relationship between the board and its adviser in management material risks faced by the fund.

11. Ibid.
12. https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf
13. Ibid.
14. See Frank J. Martens and Larry Rittenberg, *Risk appetite – critical to success: Using risk appetite to thrive in a changing world, Committee of Sponsoring Organizations of the Treadway Commission* (COSO), 2020.
15. Securities and Exchange Commission (SEC), 17 C.F.R. Parts 210 and 270 (2020).
16. SEC, 17 C.F.R. 270.22e-4.
17. Ibid.
18. Paul Kraft, *Fair valuation pricing survey, 22nd edition, executive summary*, Deloitte, 2024.
19. SEC, "SEC proposes cybersecurity risk management rules and amendments for registered investment advisers and funds," press release, February 9, 2022.

Appendix

Questions directors should consider

Investment risk

- Are the levels (and types) of investment risks that the adviser is taking with respect to the fund in line with a fund's prospectus and statement of additional information?
- How does the adviser measure and quantify the risks taken by the fund? Does the adviser have systems or resources in place to measure and manage those risks? What are those resources?
- Is there a qualified derivatives risk manager in place at the adviser and are there appropriate escalation protocols in place for the oversight and monitoring of risks associated with derivatives and other senior security transactions?
- How does the alpha generated by the investment compare to the risk-adjusted peer group performance?
- Is an appropriate benchmark (of similar risk profile) used for comparison of investment results?
- What types of reporting does the board receive regarding performance attribution? How often do directors receive these reports?
- How is drift within investment strategies monitored and evaluated?

Valuation risk

- Has the appropriate valuation designee been identified, and do they have sufficient resources to carry out their responsibilities for determining the fair value of all fund investments?
- What conflicts of interest have been identified within the valuation process and what controls have been established by the adviser to mitigate those conflicts?
- What is the role of portfolio managers and traders in the valuation process and are they excluded from voting on fair value matters?
- What are the valuation methodologies documented in the fund's valuation policies and procedures? Does the valuation designee evaluate the valuation methodologies and processes for new and evolving asset classes? For example, if a fund invests in private equity investments, what is the valuation process and how does it differ from other types of assets?
- How does the board monitor compliance with valuation policies and procedures? Has the board considered the effectiveness of controls over the valuation process?
- What constitutes a "material" valuation risk?
- Do the procedures account for changing or unusual market conditions, such as when particular markets are closed for long periods of time?
- How does the valuation designee evaluate new or current third-party pricing services, including pricing vendors, brokers, and others? How are such vendors selected for specific investments or classes of investments?
- What sort of information is provided by the fund or its advisers to third-party pricing services?
- What kind of periodic testing does the valuation designee use to test the quality of evaluated prices provided by pricing vendors?
- Does the valuation designee periodically test the secondary pricing vendor's evaluated prices?
- Do the valuation policies and procedures identify events when the board must be involved or must be notified? Are the "material" events that require board notification per Rule 2a-5 defined?
- Has the valuation designee identified key valuation indicators for each asset class that notify/inform fund directors of potential price uncertainty in the market?
- Has the board discussed with the valuation designee its expectations around Rule 2a-5's requirement for prompt notifications reporting?
- Does the valuation designee consult with pricing experts when addressing challenging or intricate fair valuation matters?
- How are issues associated with evaluating foreign securities at the close of the US stock market addressed?

Liquidity risk

- Does the adviser have a system to identify when funds are at risk of exceeding the established liquidity threshold?
- Does the adviser keep the board apprised of changes to the fund's liquidity risk management program?
- Is the adviser's report regarding the liquidity risk management program comprehensive?
- Does the adviser have protocols in place to notify the board, within one business day, if the fund's illiquid investments exceed 15% of the fund's net assets?

New product risk

- What risks do the fund's new strategies and/or new complex investment vehicles pose beyond those identified for existing products?
- How does the adviser evaluate the appropriateness of a new fund, and the risks associated with it? For example, does the adviser have a product governance committee?
- What systems, operations, personnel/skills/talent, and technology support will the new strategy or new investment require? Do existing operations and systems require enhancement to support the new strategy or investment effectively? Do third-party service providers, such as a fund administrator, pricing vendor, transfer agent, custodian, etc. have the requisite expertise, staffing, and systems to support the new product or investment strategy?

- If the fund is sub-advised, does the adviser have adequate access and transparency into the sub-adviser to perform appropriate oversight? Is the sub-adviser experienced in managing the strategy within the confines of a fund regulated under the 1940 Act, a separately managed account, or other institutional account?
- Is the new product or strategy appropriate for the fund structure? For example, would the product or strategy be more suitable for a closed-end fund or vehicle with less daily liquidity needs?
- Is the adviser able to execute the new strategy while also adhering to any existing limitations (e.g., leverage, liquidity), whether due to regulatory restrictions or policy/strategy restrictions? Are these products periodically stress tested under various historical and hypothetical scenarios?
- Do existing valuation policies, procedures, and controls address valuation risks associated with new products or strategies?
- Have additional risks specific to new products and strategies been appropriately disclosed to investors in the prospectus, fund marketing materials, and other fund offering documents?
- Has a time frame been established with goals for measuring the success of a new product?
- How will the fund board reporting need to be updated to provide appropriate oversight of these new risks?

Alternative, untraded investment risk

- Is the investment objective of the fund compatible with an allocation, given the unique nature of private markets?
- What are the policies and controls surrounding allocations to alternative investments?
- How does the adviser assess the risk levels associated with alternative, non-traded ("alternative") investments? Does the adviser have the right skills to account for, report, and value such alternative investments?
- Does the adviser have a rightsized and properly resourced due diligence team to analyze the investments?
- How will the adviser assess potential conflicts of interest given the reduced transparency related to underlying holdings?
- How are the holdings fair valued?
- Are the appropriate valuation policies and procedures in place that incorporate the methodologies around valuation of the alternative investments?
- Does the adviser have an internal valuation team able to value the investments and will the outside auditors be able to independently evaluate the valuations?
- What monitoring and review policies are in place for each alternative investment?
- What frequency of valuation will be performed?
- Based on significant events (i.e., microeconomic, industry, company specific), what is the process to update valuations on an inter-period basis (i.e., once a significant event has occurred, how quickly will a revised valuation be performed? What factors are considered? Who will perform the valuation?)?
- What is the adviser's ability to monitor for conflicts of interest in alternative investments?

Special-purpose acquisition companies (SPAC) risk

- Has the adviser performed due diligence regarding the SPAC?
- Has the adviser considered risks unique to the SPAC structure?
- Is an investment in SPACs consistent with the fund's investment objectives?
- Has the SPAC been able to execute on acquisition of a target company in the allotted time frame?
- Are there particular valuation concerns about acquiring pre-IPO securities through

ESG funds risk

- How does the adviser approach its use of ESG—as a hedge against potential investment risk or as an investment philosophy?
- How is the fund's ESG process described in disclosure documents? Is the investment process used by the fund consistent with that description?
- How is compliance with disclosure tested?
- How does the adviser consider the impact of state and federal regulatory scrutiny of ESG investments?

Technology risk

Information technology risk

- Is IT risk appropriately covered in the risk reporting provided to the fund board?
- What key IT initiatives are under consideration or underway that will impact the funds, and what data sets and information does the board receive on these initiatives and impacts?
- What is the relevant technology infrastructure, and the suitability/condition of the infrastructure, at the adviser and other key service providers?
- What key operations of the IT platform and structure have been outsourced?

- If the adviser or other key service providers are considering migrating infrastructure to a cloud service provider, is the cloud migration strategy and road map aligned with IT and organizational goals? Does management have appropriate resources in place to identify and manage incremental cloud security risks? Are these resources continually trained in the latest and greatest practices to drive secure cloud adoption? Has management considered enhancing current incident management capabilities and processes to scale for the evolving cloud threat landscape?
- Does the fund have proprietary applications that should be assessed from a security perspective (dynamic and static application security testing, secure code analysis, etc.)?
- Is there effective due diligence, monitoring, and vendor management over outsourced IT services? Are service provider and subscriber responsibilities clearly defined and does vendor management over IT services appropriately consider legal liability, insurance coverage, and roles during incidents and investigations

Cyber security risk

- Has the adviser established a risk-based cybersecurity strategy that aligns with overall business and IT strategy?
- Have cross functional leaders defined organization-wide IT risk and cybersecurity policies, standards, and procedures that are aligned with the funds' strategic and business goals?
- Has the adviser done a cyber risk assessment to understand the overall program maturity, risk, and prioritization roadmap?
- Has the adviser identified the funds' key assets and where they exist?
- Does everyone in the organization understand the adviser's cyber risk appetite?
- Does the CISO (or equivalent) have the resources necessary to manage IT/cyber risk? What training is given to employees regarding cybersecurity?
- What preparations are in place to operate during a ransomware attack, breach, or incident? Does the adviser have an incident response plan and a strong resiliency program?
- Does the adviser have cybersecurity insurance?
- When would the board be notified regarding a data breach and/or cyber incident?

Data risk

- Have data-related policies and standards for data risk identification, mitigation, and accountability been defined and established?
- Has a data governance model been constructed?
- Are the three lines of defense (i.e., front line operations, risk and compliance management, and internal audit) working in tandem to holistically identify and manage data risks?
- How are data risks defined, aggregated, reported, and monitored by the board and other management stakeholders?
- Are investments in technology solutions/platforms aligned to the fund's goals of minimizing data risks?

Model risk

- How does the adviser define models?
- How does the adviser manage model risk? Does the adviser have a robust model risk management program?
- How are model outputs validated?
- What is the difference between models that make automated investment transactions and tools used as inputs in the portfolio manager's decision process?
- Who in the organization oversees model risk, and do they have the ability and authority to effectively challenge model owners? Are models subject to independent validation prior to being put into production?
- Who reviews model recommendations prior to implementation?
- Does the adviser have a process for how model inputs can be changed?
- Are there post-implementation and annual model risk reviews?
- How does the adviser review and test third-party or vendor models?
- How often is back testing conducted on rule based and smart beta products?
- Have appropriate peers been identified for benchmarking?
- What type of regular reporting does the board receive on significant model risks, both for specific models and in the aggregate?
- Does the adviser have change management procedures and controls in place to appropriately capture and record model changes over time?
- What defines an error or incident?
- Does internal audit or a third party perform a periodic audit to determine that model risk activities, framework, and model outputs/valuations are being performed adequately based on policy?

Artificial intelligence risk

- Does the board understand how AI is deployed and utilized by the adviser? How is AI use monitored by the adviser?
- Does an inventory or catalog from the adviser and affiliated service providers exist, detailing AI usage and risk assessment categorization (e.g., high, medium, or low)?
- What data is being used to train the artificial intelligence models? Advisers must ensure that data used for training complies with privacy laws. Sensitive client or proprietary data must be anonymized or protected.

- How are data breaches being mitigated? Cybersecurity protocols must be robust enough to prevent unauthorized access to models or data.
- How does the adviser assess and monitor model fairness? Regular audits should be conducted to ensure AI outputs are equitable across demographics.
- Can the adviser explain how the artificial intelligence model reaches its conclusions? AI models should be able to be explained in plain English to enable effective compliance and oversight, particularly for decisions that affect clients or regulatory filings.
- What level of transparency does the third-party provider and/or adviser offer regarding AI decision-making? The board may inquire about key elements of the AI's decision logic to manage potential risks effectively.
- Is there a robust process for testing and validating artificial intelligence models? Models should undergo rigorous testing, including stress tests, back-testing, and scenario analysis, to ensure they perform as expected in different market conditions. Independent validation of AI models can reduce risks of internal bias or oversight, ensuring that models function properly before they are deployed.
- How does the adviser balance human oversight with artificial intelligence usage? While AI can automate decision-making, overreliance without human oversight can increase operational risk, especially in complex or unforeseen situations.
- Are there processes in place to ensure human accountability for AI outputs? Accountability frameworks should ensure that AI-driven decisions have human sign-off, especially in high-stakes decisions.
- Are model changes and updates thoroughly tested before implementation? Any updates to artificial intelligence models should be carefully reviewed and validated to prevent unintended consequences.
- Is there transparency with clients/investors regarding the use of AI? Investors may need to be informed about when AI is being used to provide recommendations or manage portfolios, especially if AI influences investment outcomes.
- Who is responsible if artificial intelligence makes an erroneous or harmful decision? Directors may wish to define clear accountability in case AI decisions lead to significant financial or reputational damage.
- What contingency plans are in place if AI systems fail? Disaster recovery and alternative strategies should be in place to manage failures in AI systems.
- Is the use of artificial intelligence overseen by a governance committee within the organization?

Operational risk

Day-to-day operations risk

- Do operations adhere to relevant regulatory requirements and guidelines?
- Are robust systems, controls, and processes in place to minimize the risk of errors?
- Do recovery plans and incident management protocols exist to enable a suitable response when events occur?
- Is there a clear distinction between director oversight and day-to-day management?
- How are conflicts of interest identified and managed to prevent conflicts from affecting operational integrity?
- Are the appropriate governance frameworks in place to ensure accountability?
- How are operational processes monitored and assessed to identify areas for improvement?
- Are tax risks adequately managed, and is regular tax testing conducted to ensure compliance and optimize tax outcomes?

Business resilience risk

- What recovery plans does the adviser or service provider have in place?
- What evidence exists to demonstrate that the adviser can respond and recover the end-to-end business service within the expected time frames? Does the adviser have insights into the infrastructure, third party and applications that the business services depend upon for efficient decisions?
- Do the relevant parties within the adviser have a clear understanding of their responsibilities? Do directors and executives understand how they will be involved and make decisions during a crisis event or disruption? Do the recovery team members have a clear understanding of their roles and responsibilities? Has the adviser simulated those? What happens if a critical third party is impacted by an extended disruption?
- Has climate risk been considered and evaluated as part of the recovery plans?
- How and how often are the strategies and playbooks tested? Are the tests designed to identify potential gaps?

Third-party risk

- How does the adviser think about its third-party risk management? How does it see the program evolving?
- Has the adviser conducted a third-party inventory that is widely available in the organization?

- How does the adviser assess its critical service providers? For example, has the adviser established a tiered approach to third-party risk management that identifies the most-critical services providers and vendors and manages the risk presented by those entities accordingly?
- How is the adviser using technology to enhance its monitoring of service providers?
- How often does the adviser review its program to identify areas of enhancement?

Next-gen TPRM

- How does the adviser think about its third-party risk management? How does it see the program evolving?
- Has the adviser conducted a third-party inventory that is widely available in the organization?
- How does the adviser assess its critical service providers? For example, has the adviser established a tiered approach to third-party risk management that identifies the most-critical services providers and vendors and manages the risk presented by those entities accordingly?
- How is the adviser using technology to enhance its monitoring of service providers?
- How often does the adviser review its program to identify areas of enhancement?

Regulatory risk

Regulatory compliance risk

- How are regulatory issues monitored and by whom?
- What information is provided to the board regarding the implementation of new regulatory requirements?
- Who ensures the adviser ensure existing laws and regulations are followed?
- How does the adviser track enforcement and regulatory actions by regulators other than the SEC, as applicable?
- What reporting do the fund directors receive to understand regulatory compliance trends and the risks that they may pose?
- How does the adviser's due diligence regarding sub-advisers monitor for regulatory compliance?

Disclosure risk

- Do the adviser, fund counsel, and others relied upon by the board have sufficient controls to determine that disclosures and statements included in fund documents are are appropriate and remain current?
- Do the adviser, fund counsel, and others relied upon by the board have appropriate controls to identify appropriate disclosures or risks as the funds engage in new investment types?

Money laundering risk

- Does the fund have a process to regularly review regulatory requirements, regulatory guidance, and recent AML enforcement actions to determine whether a fund's AML program, or its policies and procedures, should be changed or enhanced?
- Does the fund delegate aspects of its AML program to a third party (e.g., a transfer agent), and if so, does it have the appropriate oversight and metrics to demonstrate effective governance of the AML program as well as third parties that support it? Is initial and ongoing due diligence performed on the third party?
- Has the fund's administrator, transfer agent, or custodial bank been subject to an enforcement action? If so, what, if any, effect did the enforcement action have on the fund's investors?
- Is annual independent testing of the fund's AML program conducted? If so, what deficiencies or enhancement opportunities were identified in recent reports and have management action plans been developed to address them?

Strategic risk

Reputational and crisis management risk

- How are risks, risk events, or actions that may cause reputational damage identified and monitored? Does the adviser perform reputational risk sensing or intelligence gathering activities?
- Is the adviser crisis-ready and well prepared to navigate a reputational event? Are crisis response plans periodically tested and improved upon?
- How is the fund board engaged and informed of potential reputational risk events and crisis mitigation strategies?

Human capital risk

- How does the firm plan to attract top talent in a competitive market?
- What measures are the firm taking to retain top performers?
- Is the firm offering flexible work arrangements that meet the needs of its employees?
- How is the firm fostering a positive and inclusive workplace culture?
- Is the firm leveraging the latest digital tools and technologies to enhance productivity?
- How is the firm utilizing AI to improve decision-making and customer experiences?
- What investments are being made in research and development to drive innovation?
- How is the firm encouraging a culture of continuous learning and development?
- Does succession planning exist for key roles?

Deloitte.

10718050