MFDF
MUTUAL FUND DIRECTORS FORUM
The FORUM *for* FUND INDEPENDENT DIRECTORS

Mutual Fund Directors Forum

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

May 2020

Table of contents

INTRODUCTION 1

ROLE AND DUTIES OF FUND DIRECTORS

Obligations Under State Law, the 1940 Act, and the 1933 Act 2

Court and SEC Guidance 3

THE RISK MANAGEMENT FRAMEWORK

Elements of an Effective Risk Management Program 4

SPECIFIC RISK AREAS IMPACTING THE INVESTMENT MANAGEMENT INDUSTRY

Investment Risk:

- Investment Risk 10
- Valuation Risk 11
- Liquidity Risk 12
- Model Risk 13

Operational Risk:

- Information Technology Risk 14
- Cyber Security Risk 15
- Data Management Risk 16
- Business Resiliency to Manage Risks 16
- Third Party Service Provider Risk 17
- Cloud Adoption Considerations 18

Strategic Risk:

- Reputational Risk 19
- Risk Related to New Products 19
- Business Challenges and Risk 20

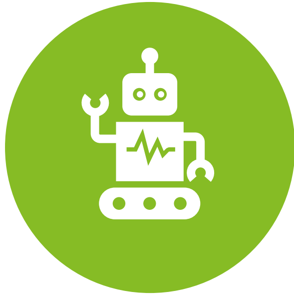
Regulatory Risk:

- Regulatory Compliance Risk 22
- Disclosure Risk 23
- Money Laundering Considerations 23

NOTES 24

MFDF RISK OVERSIGHT WORKING GROUP 25

Introduction



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

There are two primary types of risks in the investment management business – intended risks which are necessary to achieve the fund's investment objectives and create shareholder value and uncompensated or undesirable risks that are best avoided, if possible. As part of their overall oversight responsibilities to the funds, boards of directors of registered funds (hereafter referred to as "fund directors," "directors," "fund boards," or "boards") should understand these different types of risk and the policies and procedures used by the adviser to appropriately manage these risks.

An open and transparent dialogue between the fund board and the adviser and service providers about the types of risks their organizations face, their appetite for those risks, and the programs and processes in place for managing those risks can facilitate this understanding.

This paper[1] sets forth key concepts, principles and some questions that boards may find useful as they seek more information about a fund's risks.

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

The Mutual Fund Directors Forum recognizes that a "one-size-fits-all" approach to risk oversight and risk programs is not possible given the diversity among funds and fund families as well as the evolving nature of risk in a dynamic environment and industry. Consequently, when discussing the fund's risk management with the fund's adviser, directors should consider the factors relevant to their particular fund complex, such as the characteristics of the funds they oversee, the fund's investment objectives and asset size, as well as complex specific factors including complexity, disparity of fund types and number of funds. In all cases, directors should focus on risk areas where the adviser's interests conflict with the fund's interests. Directors should also seek to understand the current governance and management structures in place along with the nature of third-party service arrangements and the existing programs in place to manage those services.[2]

Role and duties of fund directors

Fund directors are responsible for understanding and overseeing how the fund's adviser manages a fund's risk, including risk management and oversight of the fund's service providers. While there are no well-defined risk management duties for fund directors, fund directors can establish a solid foundation for their legal obligations with respect to 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 investment, operational, regulatory and emerging risks affecting a fund and fund complex; and
- Risk management frameworks and processes implemented by the adviser and fund service providers to identify, manage and mitigate risk.

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 his or her actual knowledge and any knowledge he or she should have obtained in functioning as a director. Under state law, directors are generally permitted to reasonably rely on experts, including counsel, the fund's adviser, accountants and others.

The duty of loyalty means that a director owes a duty to protect the best interests of the fund and not to pursue his or her own interests or those of a third party over the interests of the fund. The duty of loyalty also encompasses the duty to act in good faith.

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

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

- Evaluating fees charged to the fund and valuing the fund's assets;[5]
- Dealing with conflicts of interest;[6] and
- Assessing third-party service providers.[7]

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 U.S. Supreme Court, the SEC and SEC staff have consistently emphasized that the fundamental obligation of a fund director is to protect the interests of a fund's investors. The SEC[9] and Supreme Court[10] have made clear that requiring a board of directors that is independent of a fund's adviser is a cornerstone of the structure developed in the 1940 Act to protect the interests of fund investors. The SEC staff has historically emphasized that, in order to fulfill their oversight role, fund directors should not be involved in day-to-day management activities of their funds.

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

- 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.
- 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.[11]

While fund directors could be tempted to become drawn into the day-to-day operations of a fund and its adviser or other service provider, 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.[12] These obligations cannot be met, nor can a fund's investment adviser execute its own responsibilities, unless the fund's directors appropriately delegate day-to-day management responsibilities to the fund's investment adviser and other third-party service providers.

Fund directors should work with the fund's investment adviser and service providers, and consult with outside experts as applicable, to understand, challenge and oversee how risks are identified, assessed and managed. In addition to consulting with the adviser's or service provider's risk management personnel, the fund's chief compliance officer ("CCO") can be an essential 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.[13] In addition, Fund directors will want to understand the scope of and leverage the internal audit function to facilitate their oversight role and duties.

The risk management framework

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

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

Investment risks, which are related to the portfolio composition, and risks related to market, credit, liquidity, and leverage among others;

Operational risks, which include risks related to people, process, and systems including technology and information/cyber security;

Strategic risks, which are those that could disrupt the objectives and assumptions that define an organization's business strategy, including risks to competitive position and strategy execution; and

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

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 directly responsible for risk management, they should understand the adviser's risk management approach, framework and program for risk identification, assessment, mitigation, monitoring and reporting. Fund directors should appreciate how the adviser tailors its risk management program to address the risks of a particular fund, as well as emerging risks.

Despite the diversity in how risk management programs are designed and implemented, most risk management programs follow a similar approach and principles, and all should be designed to identify, measure, and manage the most significant risks to within an acceptable risk appetite or tolerance level, not eliminate or even further reduce every risk. Moreover, as funds grow and evolve, their risk management programs should as well.

Regardless of the particular risk management program or model[14] that is used by the adviser or service provider, there are significant elements and processes that are characteristic of an effective risk management program as discussed in more detail in the following sections. Many of these elements and processes are endorsed by COSO or other recognized frameworks.

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. These attitudes and principles are referred to as "tone at the top" and should cascade throughout the firm to become the "tone at the middle" and then become further 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's risk philosophy and approach to risk management. While the tone at the top may be difficult to empirically evaluate, 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.

In further evaluating the risk culture at a firm, a fund director may find it helpful to determine how the risk management program 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:

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

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

- Who is responsible for risk management and what is the governance structure? Are risk managers within business units or outside of them, or both? Are there appropriate independent challenges embedded in the program? Are there controls in place to manage conflicts which may arise if the risk managers are within the business units? Is there a formal second line of defense risk function?
- What is the process for monitoring existing risks and identifying emerging risks?
- What kind of education on risk management is given throughout the organization, including to personnel outside of any dedicated risk management function?
- How are key risks, including plans to mitigate these risks, reported and challenged within the organization?
- How are control gaps or failures that result in actual incidents (i.e., the realization of a risk or risk event) addressed and reported in the organization?
- How are actual incidents considered in the assessment of related risks?
- Who determines which incidents are escalated to senior management and/or the fund board? What are the criteria for escalating those incidents? Is there periodic risk reporting to the fund directors, i.e., a risk dashboard?

The Three Lines of Defense Model

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 organization. In most organizations, a number of different teams have risk management responsibilities, including enterprise risk professionals, internal auditors, compliance officers, control assurance specialists, as well as risk and control professionals who are embedded in the operations of the business. Each of these teams has a unique perspective and role but are collectively working together to help the organization manage risk. While every organization is unique and there is no right way to organize risk functions, responsibilities should be clearly delineated, and the work coordinated, where possible. One commonly used framework is the Three Lines of Defense model. In that model, management control is the first line of defense in risk management, the various risk control and compliance oversight functions established by management are the second line of defense, and independent assurance is the third. Each of these three "lines" plays a distinct role within the organization's wider governance framework. It should be noted that the Fund's Chief Compliance Officer would have a direct line to the Board/Audit Committee.

Graphic taken from The IIA Position Paper The Three Lines of Defense in Effective Risk Management and Control *published in 2013, adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41*

Communication and Key Risk Reporting

It is important for a fund director to understand several dimensions of the adviser's risk management communications and reporting within the organization:

- Communication of risk management expectations and program across the organization;
- Key risk reporting; and
- Escalation and reporting of risk events or incidents.

In addition, the board should work with the adviser to develop a reporting protocol for how the fund board will be kept apprised of both the risk management program as a whole as well as for the reporting and escalation of specific risk events. Boards need insightful, high quality, fact-based management reports in order to be assured that the adviser is appropriately managing risk.

In addition to what communications the board receives and when, directors should examine how they organize their risk oversight responsibilities. For example, some boards may find it helpful to have a board risk committee, whereas others prefer to have risk as a board level responsibility. The decision will impact how the board communicates with management, particularly between meetings on risk-related issues.

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

- How often does the adviser discuss its general risk management program with the board? Who is responsible for these discussions? What should be included in the discussion?
- What kind of reporting does the board receive on a regular basis from the adviser?
- Does the adviser have policies and procedures that include escalation and response of incidents?
- When does the board expect to be notified of a significant risk event? What is the general process for such communication? What type of information would the board like to receive in such circumstances?
- When does the adviser communicate with shareholders and intermediaries about incidents?
- What types of risk reporting does the adviser use to manage risk that could also be of assistance to the board?
- Has the adviser established protocols with outsourced service providers for the notification of risk events? Are the protocols part of the agreement with the provider? How are the protocols monitored?
- How are risks identified and shared within the adviser?

Identifying, Assessing and Mitigating Incidents

The adviser's risk management program should include a process to identify potential risks that have been realized due to a risk management, control gap or failure. Realized risks are "risk events" or "incidents" such as a cyber breach, a significant trading error, pricing error, or exceeding/breaching an established acceptable volatility range for a fund's investment return. Fund directors should understand how the adviser identifies, captures and reports risk events and considers their impact on future risks.

Following the recognition of a risk event, the next step is identifying the reason for the incident such as a flaw in the design of policies and procedures or a failure in procedure due to human error, among other possibilities. Once the reason for the incident has been determined (if possible), the adviser can then focus on risk event remediation or response. Although there may not be an immediate response for each risk event, it may be helpful for the board to understand how the adviser responds, including the timing, personnel involved, when senior management is notified, and what information is regularly shared with the board.

Risk Appetite and Risk Tolerances

Understanding whether an adviser or service provider is managing to an appropriate level of risk across an entity is becoming increasingly important. Risk appetite and the associated risk tolerances for monitoring risk to within a firm's risk appetite are intended to support this risk management objective. Risk appetite and risk tolerances are most often used with respect to investment risk, though they can be relevant to other risk areas as well.

Understanding the risk appetite of an adviser or service provider, however, has proven 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, in defining risk appetite, different advisers may use different language and concepts. Some advisers define risk appetite in a qualitative manner (i.e., high, medium, low) whereas others may rely on more specific or quantitative measures.

Both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept, but there is an important difference between risk appetite and risk tolerance.

Risk appetite is the amount and type of risk that an entity is prepared to pursue, retain or take.

Risk tolerances are narrower and set the acceptable level of variation in achieving objectives

Simply put, while **risk appetite** is about the pursuit of risk, **risk tolerance** is about what an entity can actually cope with. Both **risk appetite** and **risk tolerance** need to be high on a fund board's agenda and are core considerations of an enterprise risk management approach.

Within an adviser, risk tolerances set expectations for variations around specific objectives. Using risk tolerances can allow management to better monitor whether the fund or fund complex is operating within its defined risk appetite and meeting its objectives.

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

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

- What is the adviser's approach to defining risk appetite for the fund and fund complex? If risk appetite is not defined, how does the adviser monitor enterprise-wide risk?
- Are key risks measured against the risk appetite and if so, how?
- Does a fund's strategy align with its risk tolerance?
- How often are risk appetite statements reviewed?
- Is there a governance process to review and approve changes to risk appetite statements?

While monitoring risk on a fund-by-fund basis is vital, such a narrow approach could expose the fund complex to added or concentrated 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. Therefore, in addition to discussing the fund-by-fund risk, fund directors should explore how the adviser monitors risk on a complex-wide basis. Additionally, when the mutual fund complex is only one of the adviser's lines of business, issues in another part of the business may impact the funds. For example, reputational risks resulting from risks arising from another area or aspect of the adviser's business may impact flows into a fund or fund complex. 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.

Control Activities

Control activities, another important element of an adviser's risk management program, are actions (generally described in policies, procedures, and standards) that help management mitigate risks in order to ensure the achievement of objectives. Control activities may be preventive, directive or detective in nature and may be performed at all levels of the organization. They could include management control functions and internal control measures in the business unit as well as oversight functions (i.e., financial controls, risk management, and compliance).

It may be helpful for a board to understand how each line of defense supports the control structure both with respect to how controls are developed and maintained in the normal course as well as when risk events occur, and control remediation that may be required as a response.

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

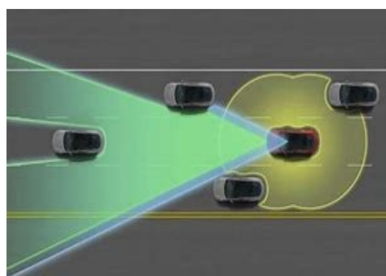
- How does the adviser develop and monitor controls for operating effectiveness?
- How are new risks integrated into the control structure?
- How are risk practices modified based on changes to the internal and external environment in which the fund operates?
- Are the controls operating effectively to manage and/or mitigate the identified risks? Is such assessment communicated to the board, and if so, how?
- Does the adviser monitor automated control activities differently from those that rely on more manual processes? If so, how does the monitoring differ?
- What is the role of the Internal Audit function in testing, overseeing and reporting on control activities?
- Does the adviser use third parties to discuss and support risks unique to a particular operation?
- How are risk events and their detection and remediation shared within the adviser and fund director?

Risk Program Evaluation

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

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

- Does the adviser maintain a risk charter that clearly highlights roles and responsibilities and the scope and focus of the risk management program?
- How does the adviser determine if the risk function is operating as intended?
- How and which risks are discussed at the risk committee(s)?
- How effective has the risk management program been in reducing operational risks?



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 timely decisions can be made to eliminate or manage the risk before it adversely impacts the adviser and/or the funds. Adaptive risk is now an emerging area that may become more prevalent as technology and risk programs evolve.

Traditionally, operational risk management was a more reactive system. Errors from risk conditions would occur and management would perform a root cause analysis to better understand why the error occurred and would assess the internal controls and operational practices to determine if they needed to be strengthened. Reactive risk review, or a post mortem 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 financial event and/or operational impact. Sound risk management practices can be designed today so that significant risk conditions are detected at their earliest stages with a rapid response capability.

To transition to an adaptive risk model framework, the adviser will first determine any predictable risks within the fund complex. That is, errors that could occur and impact the operations of the funds. By thinking proactively, risk signals can be identified. Ideally, these risk signals are digitized and can feed into a database where event detection algorithms can alert risk managers to risk conditions. Text messaging, voice messaging, and e-mail can be used to notify appropriate parties of developing risk conditions. Consequently, time and effort are then focused on dealing with the most impactful risk conditions in a timely manner while enabling more efficient use of resources.

Embedding sense and response capabilities into daily workflows and processes allows for early detection of potential business issues and can reduce business risk. There are many predictable surprises within the operations of a mutual fund complex generally. By taking an inventory of these potential risk events and reviewing the list periodically, sense and respond capabilities can be identified and built into the risk management framework.

Specific risk areas impacting the investment management industry

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

Investment Risk

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

- Trend levels of investment risk over time;
- Returns versus peer groups and benchmarks over time on both an absolute and risk-adjusted basis;
- Funds with weak performance more frequently or in a more detailed manner; and
- Unexpected performance results and/or instances of significant over/under performance.

Key Considerations for Fund Directors

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

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

Investment Risk (cont.)

Valuation Risk

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

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

The 1940 Act requires that directors determine the fair value of securities for which market quotations are not readily available. While a board cannot delegate its statutory duty, it may delegate to others, including the fund's adviser, administrator or a valuation committee, the actual calculations pursuant to the fair valuation methodologies previously approved by the directors. According to the SEC, it is incumbent upon fund directors to satisfy themselves that all appropriate factors relevant to the value of such securities have been considered and are consistently followed to determine the method of arriving at the fair value of each security.[15]

On April 21, 2020, the SEC proposed Rule 2a-5: Good Faith Determinations of Fair Value proposed rule summary, https://www.sec.gov/rules/proposed/2020/ic-33845.pdf. While the impact on fund directors would vary by complex if the rule is adopted, the rule would expressly allow the board to assign certain valuation functions to the adviser or sub-adviser. The rule envisions an active oversight model that would require fund directors actively to oversee valuation risks, fair value methodologies, pricing services, written fair value polices and procedures, testing of fair value methodologies and record retention. In addition, the rule would require certain strict reporting requirements. Comments are due July 21, 2020.

Key Considerations for Fund Directors

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

- What are the valuation methodologies documented in the fund's valuation policies and procedures? Does the adviser or other service provider evaluate the valuation methodologies and processes for new and evolving asset classes?
- Do the procedures account for unusual market conditions, such as when particular markets are closed for long periods of time?
- Who at the adviser or administrator is responsible for the execution of the valuation policies and procedures? What is the role of the portfolio manager and traders in the process?
- How are valuations tested? What kind of periodic testing does the adviser or administrator use to test the quality of evaluated prices?
- How does the board monitor compliance with policies and procedures? Has the board considered the effectiveness of controls over the valuation process?
- How does the adviser or administrator evaluate new or current pricing vendors?
- What information does the board receive regarding pricing vendors who provide the fund with evaluated prices?
- What kind of periodic testing does the adviser or administrator use to test the quality of evaluated prices?
- What are the policies and procedures of the adviser or administrator regarding price challenges? Does the board receive reporting regarding price challenges?
- What are the policies and procedures of the adviser or administrator regarding pricing overrides? Does the board receive reporting regarding overrides?
- Has the board identified conflicts of interest that could arise in the valuation process? Does the board receive information that such conflicts are addressed and managed by controls and other safeguards?
- Do the valuation policies and procedures identify events where the board must be involved or must be notified?
- Has the adviser or administrator identified key valuation indicators for each asset class that notify/inform fund directors of potential price uncertainty in the market?
- Does the adviser or administrator consult with pricing experts on difficult and/or complex fair valuation matters?
- Does the board have an adequate understanding of the fair valuation models used by the adviser or administrator?

Investment Risk (cont.)

Liquidity Risk

Ensuring that shareholders can redeem shares in an open-end mutual fund is fundamental to a fund's operation. Following liquidity disruptions in public markets, liquidity has been a key area of focus for regulators. The SEC's 2018 liquidity rule for funds[16] followed on the heels of a targeted sweep exam on fixed income liquidity that was conducted in response to a distressed debt high yield fund that suspended redemptions. Banking regulations that have impacted market making in fixed income instruments coupled with market volatility have contributed to the keen focus on this area.

While fund complexes have always been focused on liquidity, the SEC's recent rule has increased the attention on the issue. As a result, fund complexes are now required to develop liquidity risk management programs that meet the SEC's requirements, in addition to other ways that they may monitor liquidity internally. The SEC's rule 22e-4 defines liquidity risk as "the risk that a fund could not meet requests to redeem shares issued by the fund without significant dilution of remaining investors' interests in the fund." Broadly, liquidity risk includes the risk that:

- The fund does not have sufficient liquid assets to meet shareholder redemption requests in an orderly manner consistent with SEC requirements without harming remaining fund shareholders;
- Established methods to determine liquidity have not been applied consistently and/or accurately;
- Established liquidity determination methods/approaches and/or inputs are no longer appropriate, due to changing market conditions or other factors, to strictly address rule 22e-4 requirements; and/or
- The fund's valuation procedures and policies do not appropriately consider liquidity in the valuation process to achieve accurate security valuations.

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

- Approve the fund's liquidity risk management program;
- Approve the designation of an administrator or committee designated to administer the liquidity risk management program;
- Receive a report at least annually regarding the liquidity risk management program, which will include notice of any material changes in the program;
- Approve any changes to the fund's highly liquid investment minimum if the fund seeks to change the minimum when already below the established minimum; and
- Be informed within one 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 in 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.[17] 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. This scenario has two potential outcomes 1) the risk of dilution for the fund's remaining shareholders and 2) the need for good supporting documentation as the likelihood that the valuation used as a final market sale price could be subject to questions in hindsight. In addition, the lack of publicly available information on a private placement security may result in fair valuation estimates not being reliable indicators of market prices. Fund directors should understand the policies, procedures and models used to generate private equity and debt valuation estimates and how the lack of liquidity is considered.

Related Resources

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

Relevant Literature

- ICI Valuation Compendium – https://ici.org/pdf/pub_15_valuation_update_vol1.pdf
- MFDF Report: Practical Guidance for Fund Directors on Valuation Oversight – https://www.mfdf.org/news-resources/news/2012/06/28/practical-guidance-for-fund-independent-directors-on-valuation-oversight
- MFDF Report: Risk Principles for Fund Directors - https://www.mfdf.org/news-resources/news/2010/04/13/risk-principles-for-fund-directors

Investment Risk (cont.)

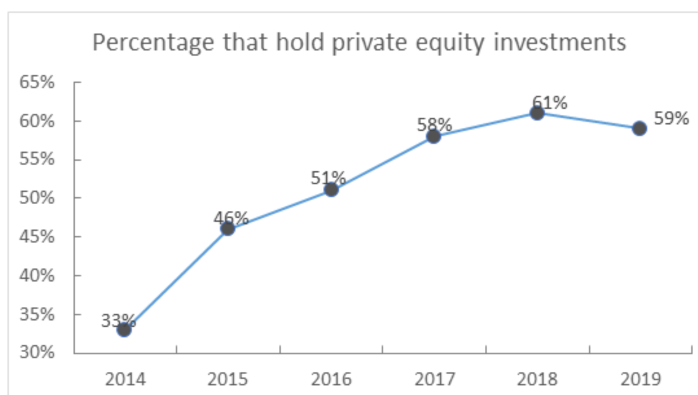
Key Considerations for Fund Directors

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

- What are the liquidity assessments and classifications in the fund's policies and procedures?
- Who is responsible for the execution of the liquidity risk management program? What is the role of the portfolio manager in the process? What is the role of the fund traders?
- How are liquidity determinations challenged? Is back testing performed?
- How does the board monitor compliance with the liquidity risk management program? Has the board considered the effectiveness of controls over the process?
- What information does the board receive regarding the liquidity process and the liquidity risk management program?
- What types of disclosures does the fund make related to liquidity and/or the liquidity risk management program?
- Can the fund use swing pricing? Short term? Long term?
- Beyond the fund's investments, what additional sources of liquidity are available? For example, are bank lines of credit in place? The ability to execute interfund lending? What are the policies and procedures governing the use of bank lines of credit and interfund lending?
- What types of systems and operating practices are in place to manage the fund's day to day liquidity risk management practices?
- Does the adviser or other appropriate service provider run mock scenario stress testing to gauge the effectiveness of controls over liquidity?
- Does the adviser or other appropriate service provider monitor concentrated investments in illiquid securities and appreciate how sales of such securities in a redemption environment may impact the fund and its shareholders?

Model Risk

With the increased reliance on technology to standardize processes, more funds rely on models in a number of areas including valuation. For example, with the increase in private equity holdings, as illustrated in the chart below, mutual funds increasingly rely on models for valuation or pricing of financial instruments. Additionally, fund advisers use models for asset selection, risk management, allocation of positions between funds, and other operational functions. Model risk is the potential risk for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model issues can lead to monetary loss, harm to clients, erroneous financial statements, improper investment or managerial decisions, or damaged reputation resulting from poorly constructed, interpreted and maintained models.



Source: Deloitte Fair Valuation Survey 17th edition – Percentage of Mutual Funds holding private equity investments

Model issues have occurred where:

- Model elements (i.e., algorithmic formulas) are not properly maintained and updated when new data becomes available
- There is a modification to existing data, models are not documented such that they can be understood by users or stakeholders (i.e., key person risk);
- Assumptions are not tested adequately resulting in faulty data inputs and assumptions; and
- Models are not validated.

Regardless of the cause, model issues and failures may potentially cost millions of dollars to investigate and remediate – causing significant erosion in organizational value, including reputational loss, regulatory sanctions, and economic and financial losses.

Investment Risk (cont.)

Key Considerations for Fund Directors

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

- How does the adviser manage model risk? Does the adviser's model risk management program include:
  - A complete model inventory and risk rating of all models used by the fund adviser?
  - Model development guidelines that include but are not limited to requirements related to data appropriateness, conceptual soundness, estimation methodologies, and documentation requirements?
  - Implementation and use guidelines, covering responsibilities of model owners and users, including but not limited to proper use of models and ongoing monitoring of model effectiveness?
  - Robust model validation process for new models as well as for substantive changes to existing models?
- Does the model make automated investment decisions or is it used as an input 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?
- How does the adviser review and test third-party or vendor models?
- 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?
- 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?

Operational Risk

Information Technology (IT) Risk

Technology enables virtually every activity at the adviser and the funds' other service providers. The reliability and the security of technology is critical. Weak controls can lead to system failures, processing errors, unauthorized transactions, and compliance breaches. Further, regulators continue to focus on the safety and soundness of data and technology in addition to compliance with laws and regulations. Ultimately, the effective management and governance of IT risk depends on both the senior executive team (including, as applicable, the chief technology officer (CTO), chief risk officer (CRO), the chief information security officer (CISO)), as well as a broad set of accountable managers from across the organization. While IT risk frameworks vary from organization to organization, effective IT risk management helps drive a practical and consistent operating model across all IT domains (i.e., IT strategy, data management, service delivery and operations, etc.) to identify, manage, and address risks.

To address technology risks, board members need not become experts in IT, but they do need to understand the IT landscape well enough to oversee management's efforts.

Key Considerations for Fund Directors

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

- What is the relevant technology infrastructure at the adviser and other key service providers? Do they operate on current versions of industry accepted applications? What key operations of the IT platform and structure have been outsourced? Offshored?
- What key IT initiatives (purchases, projects, implementations) are under consideration or underway?
- Do business and IT work collaboratively in development of new systems and or applications?
- Is there effective due diligence, monitoring and vendor management over outsourced IT services?
- Have thresholds been defined for IT risk situations to be brought to the board's attention, including significant IT investments, proposed vendor contracts with significant IT risks, and certain risk events, such as cyber breaches, system outages, or items triggering regulatory notification?
- How does the board organize itself to oversee technology risk?
- Does IT risk have a standing space on the board agenda? Topics could include top IT risks and vulnerabilities, emerging IT risks, IT risk management investments, and IT program management initiatives.

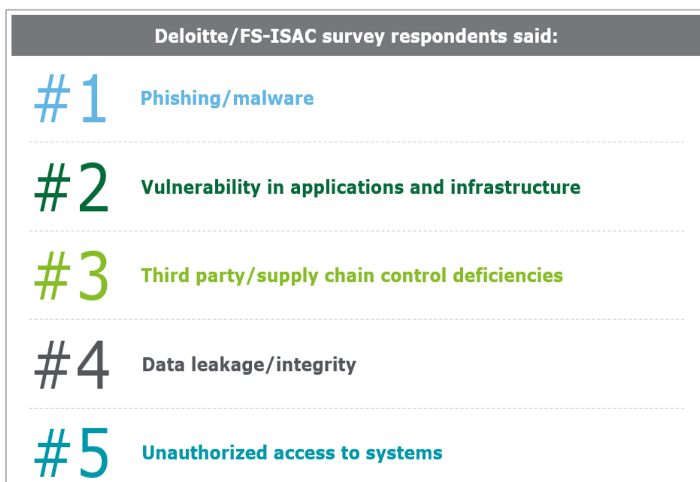
Operational Risk (cont.)

Cyber Security Risk

The SEC staff has consistently indicated that cybersecurity is a priority in their examinations of market participants, including advisers. In their assessment of how firms prepare for a cybersecurity threat, safeguard customer information, and detect potential identity theft flags, the SEC 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.

Accordingly, advisers should assess whether they and the funds' service providers have measures in place that are designed to mitigate their exposure to cybersecurity risk. The reality is cyber threats evolve quickly and perfect security is impossible. Advisers should have plans in place and capabilities to draw upon to allow for a rapid response and to mitigate the impact if and when a cyber attack occurs.

A recent survey[18] conducted jointly with the Financial Services Information Sharing and Analysis Center (FS-ISAC), reported the top 5 cyber threats. The threats identified by respondents are summarized in the chart below.



Key Considerations for Fund Directors[19]

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

- What are the greatest cyber risks to the fund(s) and how are those risks anticipated, managed and mitigated by the adviser and/or other service providers?
- Has the adviser inventoried the basic cyber risks that are inherent in the applications and systems within their span of control?
- Is the accountability and budget necessary for the creation, implementation, enforcement and updating of an integrated cyber risk management program clearly understood at the executive level?
- Does the overarching cyber risk program include all the domains of a recognized standard (such as the National Institute of Standards and Technology ("NIST")) and is it evaluated by an independent third party on a regular basis?
- Does the management team that addresses cyber risks include senior representatives from executive business leadership, IT, legal, risk management, public relations, compliance, and audit?
- Is each component of the cyber risk management program documented, frequently tested and periodically evaluated by independent experts? If so, what are the results of that testing and audit? Are the results of the evaluation used to drive IT & IT security investment decisions?
- Are the protocols for reacting to a cyber-risk crisis when it occurs well defined and broadly understood? Are they practiced through simulation exercises?
- Does the adviser have a plan for communicating with fund investors and other stakeholders, the board, regulators and the media in the event of a cyber breach, either at the adviser or a service provider?
- Do employees have access to regular education relating to cyber risks?
- Is the firm's cyber risk mitigation program adequately staffed and funded?
- What insurance coverage is available to the fund and its directors and/or the fund's service providers in case of a cyber-risk incident? Is that coverage adequate in scope and amount?
- How does the board oversee cyber security related issues? Is cyber risk oversight assigned to a committee? What types and frequency of reports are appropriate?
- How frequently is the board provided updates on the firm's progress in mitigating the different types of cyber risks? What cyber events are immediately reported to the board? Is there an operational monitoring function (e.g., a Cyber Security Operations Center) at the adviser?
- How does the board stay abreast of relevant cyber security issues? Would the board benefit from bringing in an outside cyber security expert for educational purposes? Should the board consider attending other informational sessions or conferences?
- Does counsel have a checklist of security requirements for third parties (e.g. cloud, Software-as-a-Service providers, etc.)? Has counsel reviewed contracts with outside parties to consider appropriate risk allocation for cyber events?
- What are the cyber risk due diligence practices for critical service providers? Are those diligence expectations periodically discussed and reemphasized with those critical providers?
- Is the firm's cyber risk mitigation program adequately staffed and funded? How frequently is the board provided updates on the firm's progress in mitigating the different types of cyber risks?

Operational Risk (cont.)

Data Management Risk

Ineffective data management can cause a number of issues, including financial fraud, accounting and regulatory reporting issues, and loss of investors' trust. Additionally, regulatory agencies are expressing strong interest in data management capabilities, given that fund operations depend on reliable, accurate, and timely data. In addition, organizations are increasingly combining external data with internal data, adding new layers of complexity to data management and, potentially, new risks. Rigorous data management capabilities rest on data governance or policies, and procedures that support accuracy, reliability, and timeliness of data, and clarify data ownership, uses and alteration. Controlled creation, transformation, storage, and disposal of data is central to the concept of data integrity.

Key Considerations for Fund Directors

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

- What are the adviser's data management and data governance policies and standards?
- Are critical data elements identified in key applications?
- How is data governance integrated with IT processes such as the systems development lifecycle, architecture reviews, and the like?
- How much relative effort does the adviser or service provider dedicate towards the prevention versus detection versus remediation of data and/or cyber risks?

Business Resiliency to Manage Risks

Risk management programs also must consider how the business will continue in the event of a significant disruption. Disruptions including pandemics, disasters, emergencies, an outage at a critical service provider, or other events pose significant risks to a fund and its investors. As a result, business continuity planning is crucial. Given the potential loss to fund shareholders, the SEC staff has emphasized the importance of business continuity plans ("BCP") for funds, providing guidance on important considerations in assessing a complex's ability to continue operations following a business disruption.[20] The staff noted the importance of understanding critical service providers' "business continuity planning and disaster recovery protocols" as well as "how the fund complex's own BCP addresses the risk that a critical third-party provider could suffer a significant business disruption."[21]

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

Organizations may prefer to develop broader resilience programs which include end-to-end business recovery and continuity, including the people, process and systems needed to support critical business services and operations. These programs also take into account the services performed by critical third parties. With technology enabling virtually every business activity at an adviser and the other service providers to funds, planning to make IT systems resilient to disruptions and outages is vitally important. As when assessing risks in many areas, the focus should be on the technology that supports the fund's most critical business processes.

A BCP could include:

- A programmatic approach to building scalable and repeatable resilience processes, as well as response and recovery capabilities;
- Rigorous simulations and testing to prepare business leaders in the event of a business or technology disruption or crisis; and
- Pre-and post-crisis event intelligence to predict and monitor crisis events and support timely decision making.
- Plans to address the risk of a critical service provider, complete understanding of the extended enterprise, dependencies on data and shadow NAV capabilities.

Operational Risk (cont.)

Third Party Service Provider Risk

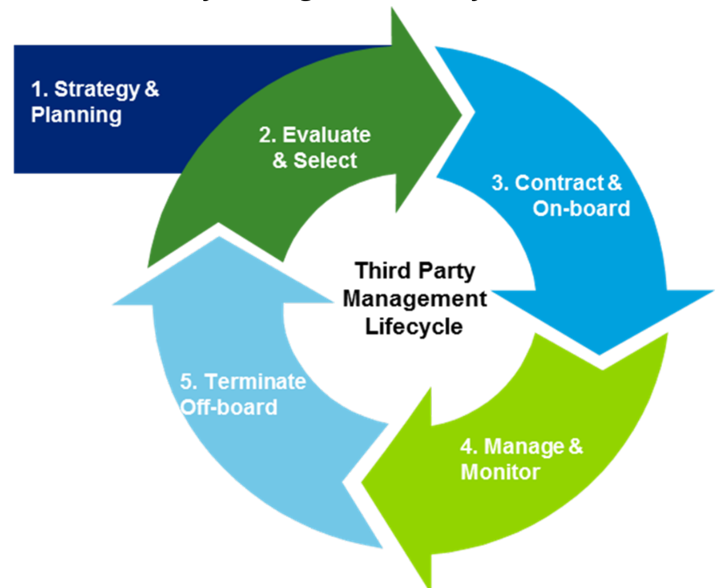
The mutual fund industry continues to increase its reliance on third parties to perform a variety of critical activities, including those performed by sub-advisers, fund administrators, custodians and accounting agents, transfer agents, sub-accounting firms, and other intermediaries. The chart below illustrates how complex these relationships can be.

A typical investment management organization may use thousands of third parties to meet its business objectives. Do you know who you are doing business with?

Investment Manager
Core Service Providers
Sub-Adviser
Accounting/ Audit Firm
Data Providers
Prime Brokers
Transfer Agents
Distribution
Joint Ventures
Operations Support
Proxy Voting Providers
Corporate Actions Providers
Private Placement Agencies
Fund Admin
Compliance Firms
Pricing Vendors
Valuation Specialists
Call Center
Client Support
Office Products
Waste Disposal
Cleaning
Facilities
Human Resources
Recruiting
Contractors
Benefits Providers
Payroll Processing
Marketing
Advertising Agency
Media and Sales
Insurance
Legal
Technology Providers
Infrastructure & Application Support
Contractor
Hosted Vendor Solutions
Disaster Recovery
Licensed Vendor Solution
Hardware Lease

The SEC continues to emphasize the importance of adequate third-party oversight as noted through its staff 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 cyber security.[22]

The Third Party Management Lifecycle



Operational Risk (cont.)

While third party oversight is not new, the way in which it is conducted is evolving. Advisers are shifting towards implementing structured programs used to support the risk management program which can assist the adviser in identifying third party risks before they impact the organization. In considering how to manage third parties, the adviser may consider the third party management lifecycle (pictured above) along with operating components necessary to manage the program effectively, including appropriate governance, policies, controls/standards, reporting, and supporting tools. Without an effective third-party management program, the fund complex can be exposed to increased risks, including:

- Entering into contracts that incentivize a third party to take risks that are detrimental to the fund or its investors, in order to maximize the third party's revenues;
- Lacking an oversight structure within the client service teams or other groups to oversee work that has been off-shored;
- Failing to effectively weigh risks and direct and indirect costs involved in third party relationships when evaluating service options;
- Failing to negotiate an effective service level agreement ("SLA") with the third-party;
- Failing to perform adequate due diligence and ongoing monitoring of third-party relationships including entering into contracts without assessing the adequacy of the third party's control environment exposing risks such as data privacy;
- Engaging in informal third-party relationships without contracts or with contracts lacking appropriate risk allocation among the parties;
- Failing to identify critical services to the fund that are not supported by an effective business resiliency plan (i.e., alternative providers);
- Failing to contemplate 4th party contracts for significant services;
- Failing to clearly identify, discuss, and document expectations for the communication of risk events and service level requirements.

Key Considerations for Fund Directors

Directors may find the following questions helpful as they consider a fund's third party service provider risk:

- Is the adviser aware of the particular risks presented by each of its service providers?
- Does a collaborative, trusting relationship exist with the service provider?
- Does the adviser know which third parties are performing critical activities and are these services monitored on a continuous basis?
- Who is responsible for the governance and oversight of third parties? Is there a dedicated owner or group for third party risk?
- Are the oversight practices (i.e., internal control review, site visits, SLA monitoring, etc.) commensurate with the level of risk the third party presents?
- How is third party risk and the oversight of third parties communicated to the board?
- Does the adviser have mechanisms to manage and track third party performance and contract compliance, including aggregate performance and trends over time?
- Does the adviser have alternative service providers in the event that the adviser would like to make a change?
- How is the information relayed to the fund's risk managers? The third party's risk managers?
- Does the adviser have an "on-boarding" process to initiate a third-party business arrangement?
- How will evolving technologies, market trends, or disruptive forces present opportunities and challenges to the fund's third-party relationships?
- How does the adviser or third party service provider oversee fourth party servicers? Does the adviser have any controls on such engagements?

Cloud Adoption Considerations

Public cloud services from the likes of Amazon (AWS), Microsoft (Azure), Google (GCP) and others offer organizations new IT capabilities that can differentiate their business and can often be less expensive than traditional on-premise infrastructure. In addition, more advisers are considering the risk and reward of a private and/or public cloud strategy. Advisers may find cloud services allow them to leverage emerging technology to create competitive advantage, reduce IT expenditure or both. However, as the value of data that resides in public cloud continues to rise, the efforts and sophistication of adversaries is ever-increasing as well. Accordingly, financial services companies must balance speed and agility with governance and control to safely realize public cloud benefits.

Strategic Risk

Reputational Risk

Reputational risk can be viewed as a loss of trust in the brand of the fund or an increase in negative perception of the brand that can lead to negative publicity, loss of revenues, asset withdrawals, loss of clients, and loss of key talent. Reputational risk can arise in a number of different ways, including from not appropriately managing a standalone investment, operational or regulatory risks such as making investments in controversial industries, technology platform failures, or cyber security breaches. While reputational risk is not a new topic, the speed and reach of social media posts have increased the potential occurrence or impact of this risk. As such, many advisers are now developing programs to focus on reputation to manage these risk events more proactively and to be better prepared for a potential crisis management situation.

Key Considerations for Fund Directors

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

- Is reputational risk integrated into the fund's risk management framework?
- How are risks, events, or activities that can give rise to reputational damage identified?
- How does the adviser stay apprised of the key stakeholders' opinions of the fund complex?
- How is the board informed of events or incidents that occur outside the purview of fund complex but that may cause reputational damage (e.g., an issue at an affiliate, another line of business of the parent, etc.)?
- How does the adviser monitor reputational risk (such as through customer surveys, media monitoring, adaptive risk monitoring, etc.)?
- Is reputational risk explicitly considered during new investment, product, or business evaluation and approval process?
- Is reputational risk explicitly considered during evaluation and monitoring of third-party relationships?
- Does the fund have crisis management plans in place that are periodically tested (i.e. via desktop or war gaming exercises)? How are test results reported to the board? What are the escalation points in the fund enterprise to review and respond to reputational brand issues?
- Does the adviser perform "risk sensing" to determine risk considerations related to its brand (i.e., what do people say about the adviser, what are the risk considerations related to competitors' challenges)?

Risk Related to New Products

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

Key Considerations for Fund Directors

Directors may wish to consider the following relating to the risk of new products:

- What risks do the fund's new strategies and/or new complex investment vehicles pose? Is the new strategy/investment appropriate for an open-end mutual fund structure? Does fund adviser have the right resources, controls and risk capabilities to manage risks at the time of the change/launch?
- If the fund is sub-advised, is the sub-adviser familiar with 1940 Act requirements? 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 mutual fund regulated under the 1940 Act?
- Has the adviser ever managed money before under a similar proposed strategy, such as in a separately managed account or other institutional account?
- What is the potential incremental impact or risk, if any, on the overall risk profile of the fund adviser?
- If the strategy requires leverage, or the new investment introduces leverage into a portfolio, are controls in place to manage and measure leverage?
- Is the adviser able to execute the alternative strategy while also adhering to any limitations on leverage, whether due to regulatory restrictions or policy / strategy restrictions? Are these products periodically stress tested under various historical and hypothetical scenarios?

Strategic Risk (cont.)

Risks Related to New Products (Cont.)

- What systems, operations, personnel, and technology support will the new strategy or new investment require? How may existing operations and systems be enhanced to support the new strategy or investment effectively?
- Alternative strategies may also introduce new operational functions, such as collateral and counterparty management. If this is the case, how will these functions be supported from a staffing and workflow perspective?
- Are there scale limitations on the adviser's ability to handle a new strategy or investment type?
- If illiquid securities are involved, are effective controls in place for measuring liquidity and meeting regulatory liquidity requirements?
- Are the fund's valuation policies, procedures and controls sufficient to support the investments contemplated by the new strategy or are changes required?
- Are the new strategies accurately described to investors in the prospectus, fund marketing materials and other fund offering documents? If a fund begins to invest heavily in a new type of investment, has that new investment risk been disclosed to shareholders?
- Are risk disclosures consistent between the fund prospectus, marketing materials and financial reporting?
- Can existing systems and personnel support these new types of investments?

Business Challenges and Risk (including Distribution/Channel Risk)

Description of the Risk

The investment management industry is in the midst of unprecedented forces that are challenging traditional industry norms, adviser operating models and adviser profitability. All aspects of how to grow, run and serve the investment management industry need to be evaluated with a strategic lens to enhance long term success. The adviser's strategy will focus on all aspects of the business including product manufacturing such as launching separately managed accounts, interval funds, ETFs, operations that support the business, the changing distribution landscape, talent acquisition and retention and the future of work. Technology is likely to be a significant factor in all of these strategic considerations. In addition, how people work, where they work, and the real estate and space floorplan (such as open offices rather than individual offices) is also likely to dramatically change in the next few years. As advisers change; who they hire and what skills they bring to the table (such as data and technology skills), the demand and race for such skills, and the potential shortage of talent and resources will be evermore competitive. Pace of change itself is a risk that the adviser is unable to respond fast enough to fundamental shifts occurring in the business landscape. Fund directors are not responsible for the adviser's strategy, however having an open and collaborative dialogue will be key to the director's oversight of the funds in the complex as well as a fund directors ability to understand any conflicts of interest that might arise. Directors should be comfortable that the adviser can effectively manage the funds and its responsibilities to the fund shareholders.

Strategic Risk (cont.)

Key Considerations for Fund Directors

Directors may wish to consider the following relating to business challenges and risk:

- As part of the 15(c) process, what has been the trendline on the adviser profitability? Has the adviser experienced fee compression across its product line?
- What disruptive forces (competitors, technology, regulatory, distribution channels) are the focus of the adviser?
- What are the new products, investment or structures that the adviser is considering? What is the timing of such launches? Have the implications to the existing product line up been considered?
- Has the adviser introduced technologies such as artificial intelligence, machine learning and the use of alternative data into the investment process? What have been the results to date? What control and audit activities have been developed to oversee and manage potential risk inherent in these technologies and the use of alternative data?
- Is the adviser planning or advancing its global investment and distribution capabilities (i.e., China, India, South America)? What added controls and resources have been added to oversee and manage the potential risks of global expansion? How does that expansion impact the adviser's ability to serve the funds?
- What changes to the adviser operating model are underway? Is the adviser considering any cost cutting/headcount reductions? What are the implications on the adviser's management of the funds of these decisions?
- Has the adviser considered the outsourcing of noncore functions to third party providers (front, middle, back office)? Why or why not?
- What changes has the adviser experienced in its distribution channel(s)? Are there alternative viable distribution options to grow the business? Can improvement be made to the customer experience?
- What investment is the adviser making in technology, people and process to enhance the customer experience? How have these impacted fund flows?

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

Regulatory Risk

Regulatory Compliance Risk

Regulatory compliance risk includes both the risk that the fund's adviser fails to comply with regulatory requirements, and the associated risk of fines, litigation costs or enforcement actions by regulators as well as the risk of new regulations or interpretations that may impact the functioning of the fund or the adviser.

The current regulatory environment is dynamic and increasingly complex. Each new regulation and interpretive position brings with it the possibility of new requirements that may directly affect the types of risks the board should oversee, as well as how boards carry out their existing oversight responsibilities. In addition to regulations that directly relate to funds, other regulations may have a profound impact on the fund industry as well. An increasingly global industry also has added to the complexity of overseeing regulatory risk management efforts, as foreign regulatory or legislative actions may impact the operations of U.S. funds or their advisers.

Evolving regulation impacts a fund's internal resources, compliance and internal controls, outsourced services providers, and a fund's systems and technology. For example, a changing regulatory environment may add significant compliance costs which are either absorbed by the adviser or passed onto investors through 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), SEC enforcement activity against a fund can be costly, both in terms of the time and money necessary to defend against a regulatory action as well as possible reputational harm.

Increasingly, directors are being held accountable for breakdowns in a fund's compliance with regulations.[23] Regulators view the boards as essential in protecting the interests of shareholders. In the past, directors have been held accountable by the SEC for breakdowns in both the advisory contract renewal process and in fair valuation.[24] The risk that the board's actions will be reviewed in connection with regulatory matters is ever present and leading to legal and/or litigation risk.

Key Considerations for Fund Directors

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

- Does the adviser have a documented process for monitoring regulatory developments or is the process managed informally?
- Has the adviser demonstrated its ability to respond to changing regulatory requirements? Has the adviser considered both the impact of individual regulations as well as the cumulative effect of changing regulatory expectations?
- What mechanisms are in place to provide the board with appropriate education and information regarding regulatory developments?
- Do the fund's policies and procedures adequately address the unique risks and challenges posed by each fund in the complex?
- How does the CCO monitor the fund's policies and procedures? What reports does the board receive about the CCO's testing?
- Does the CCO perform a risk assessment (factoring inherent and control risk) of fund policies and procedures in order to prioritize resources and compliance testing on areas deemed high risk?
- How are service providers monitored to determine whether their activities meet regulatory requirements? What type of information does the board receive regarding a service provider's compliance?

Regulatory Risk (cont.)

- Has the adviser demonstrated its ability to respond to changing regulatory requirements? Has the adviser considered both the impact of individual regulations as well as the cumulative effect of changing regulatory expectations?
- Does the fund complex engage a third-party firm to assess the adequacy of its compliance program relative to current regulations?
- What type of project management and review structure is in place to effectively manage new compliance initiatives? Is there a defined process for periodically assessing the adequacy of compliance resources?
- Does the CCO sit on the adviser committee structures acting as a non-voting member, providing consultation and advice?

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 untrue statements. Thus, directors need to be aware of the risk that disclosures and statements could be made in fund documents that are not true.

The SEC has pursued enforcement actions against fund groups for disclosures that have failed to properly inform shareholders of potential risks. In certain cases, these actions were based on a lack of disclosure regarding how a fund's returns would change as the fund grew, the impact of IPOs, and pricing policies. Most recently, the SEC has stressed the importance of adequate disclosures given the current health and economic crisis.

Key Considerations for Fund Directors

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

- What are the adviser's procedures for updating fund documents and adding new disclosures?
- Does the adviser have a disclosure committee? Does the committee oversee a sub certification process that includes key business and management participation to ensure all disclosure are captured?
- Who at the adviser is responsible for the updating of fund documents and disclosures?
- How are new disclosures reviewed and approved? What is the role of counsel?
- How does the board monitor updates to disclosure?
- Does the adviser perform a periodic update and assessment of all disclosures that includes an analysis of peer fund disclosures? Are disclosures reviewed for consistency between marketing and sales documents and fund financial statements?

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

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

- Monitoring and identifying suspicious activity, and timely reporting it;
- Explicit processes for due diligence for foreign correspondent accounts;
- Various reporting and recordkeeping requirements,

Key Considerations for Fund Directors

In evaluating a fund's AML policies, directors of funds with particular risks in this area may wish to ask the following questions:

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

Notes

1. This report has been reviewed by the Forum's Steering Committee and approved by the Forum's Board of Directors, although it does not necessarily represent the views of all members in every respect. The Forum's current membership includes over 887 independent directors, representing 122 fund groups. Each member selects a representative to serve on the Steering Committee. Nothing contained in this report is intended to serve as legal advice. Each fund board should seek the advice of counsel for issues related to its individual circumstances.
2. As the board appreciates the structure of its particular fund complex, the adviser may take the lead on particular items, while other service providers may take the primary responsibility for risk management of an item in other complexes. Therefore, in some instances the paper may refer to an adviser taking the lead in a particular risk area where another party performs the risk function in a particular complex.
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 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 staff has explicitly stated, "directors play a critical role in policing the potential conflicts of interest between a fund and its investment adviser[]" and the SEC has concurred, indicating that "[t]o be truly effective, a fund board must be an independent force in fund affairs rather than a passive affiliate of management. *Interpretive Matters Concerning Independent Directors of Investment Companies*, 1940 Act Release No. 24083 at 3 (Oct. 14, 1999) ("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 U.S. Supreme Court held that a mutual fund's investment adviser could not be found liable pursuant to an anti-fraud provision of the Securities and Exchange Act of 1934 for misstatements in the fund's registration statement because the adviser did not "make" the statements at issue in the case. The Court ruled that only those who "make" misstatements can be liable, and the Court expressly limited the provision to reach only those who have "ultimate authority over the statement" and those to whom the statement is publicly attributed. While *Janus* did not significantly modify the regulatory framework for registration statement liability, particularly as it relates to fund directors, the case served as a reminder of the importance of a director's role in overseeing a fund's public disclosure.
9. The SEC indicated, for example, when requiring that a fund's board conduct a self-assessment of its effectiveness, noted that the requirement was designed to strengthen the effectiveness of mutual fund boards as the primary protector of fund shareholders' interests, and that the self-assessment process should focus on strengthening directors' understanding of their role. *Investment Company Governance,* 1940 Act Release No. 26520 at 7 (July 27, 2004) ("Fund Governance Adopting Release") (note: two of the governance provisions adopted in this release were vacated by *U.S. Chamber of Commerce v. SEC*, No. 05-1240, 2006 U.S. App. LEXIS 8403 (D.C. Cir. Apr. 7, 2006). Industry groups have similarly elaborated on this point by advising mutual fund boards to analyze whether board members understand and respect the differences between the board's policymaking and oversight roles and the adviser's operating roles. *See, e.g.,* Report of the Mutual Fund Directors Forum, *Practical Guidance for Mutual Fund Directors: Board Governance and Review of Investment Advisory Agreements* (Oct. 2013), http://www.mfdf.org/images/Newsroom/MFDF_Practical_Guidance_Oct2013_web.pdf. *See also* Independent Directors Council Task Force Report, *Board Self-Assessments: Seeking to Improve Mutual Fund Board Effectiveness* (Feb. 2005), http://www.idc.org/pdf/ppr_idc_self-assessments.pdf. The SEC staff has explicitly stated, "directors play a critical role in policing the potential conflicts of interest between a fund and its investment adviser" and the SEC has concurred, indicating that "[t]o be truly effective, a fund board must be an independent force in fund affairs rather than a passive affiliate of management." *Interpretive Matters Concerning Independent Directors of Investment Companies*, 1940 Act Release No. 24083 at 3 (Oct. 14, 1999); Fund Governance Adopting Release at 3.
10. *See Burks v. Lasker*, 441 U.S. 471, 482-85 (1979).
11. *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.
12. *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.
13. For more information on the CCO's role, *see The Board/CCO Relationship,* available at http://mfdf.org/images/Newsroom/Board-CCO_Relationship._4.2015.pdf.
14. Two of the more common risk management frameworks include COSO and GARP. COSO is a common framework for enterprise risk management. *See*, the Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework, Executive Summary*, September 2004 (available at http://www.coso.org/documents/coso_erm_executivesummary.pdf) for more details on the COSO framework. The Global Association for Risk Professionals (GARP) also provides a commonly used framework for enterprise risk management.
15. See Accounting Series Release 118.
16. *See Investment Company Liquidity Risk Management Programs*, 81 FR 82142 (November 18, 2016).
17. Section 2(a) (41) of the 1940 Act requires directors to determine the fair value of securities for which market quotations are not readily available. See "Valuation Risk for Mutual Funds" above.
18. Deloitte – FS-ISAC benchmarking survey 2018,2019,2020, Deloitte Center for Financial Services analysis, https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html and Dbriefs conducted https://www2.deloitte.com/us/en/pages/dbriefs-webcasts/events/june/2020/dbriefs-state-cybersecurity-financial-institutions.html
19. As funds typically outsource operations and other activities to the fund's adviser (and/or other service providers), many of the questions are intended to be directed to the adviser (or other service provider).
20. *See IM Guidance Update No. 2016-04*, June 2016, available at https://www.sec.gov/investment/im-guidance-2016-04.pdf (IM Guidance Update). The SEC also has proposed a rule that would require investment advisers to adopt business continuity and transition plans. *See Adviser Business Continuity and Transition Plans*, SEC Release No. IA-4439, available at https://www.sec.gov/rules/proposed/2016/ia-4439.pdf.
21. The Reg Flex agenda for 2019 rulemaking was published in the *Federal Register* on August 7, 2018, available at https://www.reginfo.gov/public/do/eAgendaMain?
22. *See, e.g.,* IM Guidance Update. *See also 2020 Examination Priorities*, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission,. https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf
23. Andrew J. Ceresney, Director of the SEC's Enforcement Division recently stated, "as the first line of defense in protecting mutual fund shareholders, board members must be vigilant". *SEC Charges Investment Adviser and Mutual Fund Board Members With Failures in Advisory Contract Approval Process*, SEC Press Release, 6/17/15, http://www.sec.gov/news/pressrelease/2015-124.html
24. *See SEC Charges Investment Adviser and Mutual Fund Board Members with Failures in Advisory Contract Approval Process,* Press Release, 6/17/15, http://www.sec.gov/news/pressrelease/2015-124.html. *See also In the Matter of J. Kenneth Alderman, CPA; Jack R. Blair; Albert C. Johnson, CPA; James Stillman R. McFadden; Allen B. Morgan Jr.; W. Randall Pittman, CPA; Mary S. Stone, CPA; and Archie W. Willis III,* available at faith, willful misfeasance, gross negligence https://www.sec.gov/litigation/admin/2013/ic-30557.pdf.

Mutual Fund Directors Forum Risk Oversight Working Group

Elizabeth Acton	Independent Director, Fidelity Fixed Income and Asset Allocation Funds
Barry Barbash	Senior Counsel, Willkie Farr & Gallagher LLP
Barbara Baumann	Independent Director, Putnam Funds
Joe Carrier	Chief Risk Officer, Legg Mason, Inc.
Robert Chersi	Independent Director, Thrivent Funds
Anne Choe	Partner, Willkie Farr & Gallagher LLP
Suzanne Christensen	Chief Risk Officer, Invesco
Krissy Davis	Risk & Financial Advisory Partner and Investment Management Practice Leader, Deloitte
Brian Gallagher	Independent Director, Columbia Threadneedle Funds
David Gordon	Managing Director and Head of Risk, John Hancock Investment Management
Paul Kraft	Partner and US Mutual Fund & Investment Adviser Practice Leader, Deloitte
Ken Leibler	Independent Director, Putnam Funds
Hassell McClellan	Independent Chair, John Hancock Funds; Independent Director, Virtus Funds
Garry Moody	Independent Director, AB Funds
Charlie Rizzo	Chief Operations Officer, Americas and EMEA, John Hancock Investment Management
Erik Sirri	Trustee, Natixis Funds, Loomis Sayles Funds, and Natixis ETFs
Greg Weaver	Independent Director, Goldman Sachs Funds

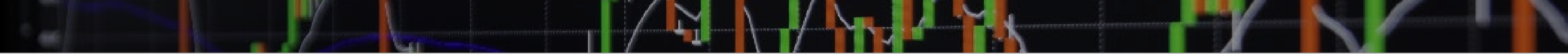
In addition, the following Deloitte professionals provided assistance and content to the overall success of this whitepaper:

- **Maria Gattuso**, Risk & Financial Advisory Principal
- **Joshua Hanna**, Risk & Financial Advisory Principal
- **Ryan Hittner**, Risk & Financial Advisory Managing Director
- **Bryan Morris**, Audit Partner
- **Mark Nicholson**, Risk & Financial Advisory Principal
- **Bruce Treff**, Risk & Financial Advisory Managing Director

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2020 Deloitte Development LLC. All rights reserved.



0
10
20
30
70
80
90