Risk Principles for Asset Managers

Prepared by The GARP Buy Side Risk Managers Forum

September 2015

Risk Principles for Asset Managers:
Table of Contents

1 Introduction

The Buy Side Risk Managers Forum (BSRMF) is composed of heads of risk management and chief risk officers from investment management and advisory companies. These include money managers offering mutual funds, managed accounts and other investment products. The forum's membership includes asset management firms operating in the U.S. and worldwide and focused on retail, high net worth and institutional clients.

The Global Association of Risk Professionals (GARP) is an association for risk managers, with a mission to advance the risk profession through education, training and the promotion of best practices globally. As part of its global efforts, GARP facilitates and supports objective and non-partisan dialogue between regulators, practitioners and leading academics to collectively and collaboratively address important risk issues.

In keeping with both groups' shared mission to explore and to define best practices, GARP together with the BSRMF has prepared this document setting out general principles of good risk management.

These principles draw on the experience and expertise of BSRMF members. As such, they reflect a long-term grounding in the investment management industry's risk practices while building upon and updating previous work by the forum, notably the Risk Principles for Asset Managers of February 2008. (http://www.garp.org/#!/buy_side_risk_managers_forum/). GARP and the BSRMF would like to specifically acknowledge Capital Market Risk Advisors (CMRA), whose substantive work on the original Principles provides a material basis for this revision.

Over the decade prior to that document's publication, the financial services industry's understanding of risk had evolved through, and been affected by, such market-shaking events as the Asian currency crisis and collapse of Long Term Capital Management, the September 11 attacks and the dot-com bubble. By late 2008, an explosion of subprime debt and derivatives products had precipitated an unprecedented global financial crisis and, in turn, a wave of regulatory reforms that, midway through the century's second decade, remain at various stages of implementation around the world.

Accompanying this new and still developing regulatory environment — and resulting from it — are structural changes in financial markets, new sets of competitive challenges and opportunities, and the imperative of heightened awareness of a multiplicity of credit, market, operational, counterparty, liquidity and other classes and subclasses of risks. It is with a view toward this rapidly changing and uncertain business and financial climate that these principles for buyside risk management have been drafted.

As fiduciaries, buy-side firms are entrusted with making decisions directly impacting the financial well-being of sovereign nations, institutions and individuals throughout the world. Decisions made by firms on behalf of clients can directly impact a corporation's ability to meet payroll, an individual's ability to retire or an insurance company's being able to pay claims. Buyside firms have a legal obligation to act in the best interests of their clients, to treat all clients fairly and to meet a very high standard of care. Thus buy-side risk management practices should be constructed and executed with fiduciary obligation as the overarching principle.

1.1

Regulation and Evolving Standards In Perspective

Since the crisis of 2008-'09, much has changed in the world in which the buy side operates. Only relatively recently has it been subject to regulatory scrutiny on the global, or systemic, scale to which banks had long been accustomed — in some cases due to the affiliations of asset managers with banking companies. However, risk management, regulatory compliance and oversight — and the risks accompanying those functions — are hardly new to the independent investment management industry.

One early statement of self-governing principles was *"Risk Standards for Institutional Investment Managers and Institutional Investors,"* produced by the Risk Standards Working Group in 1996 (http://www.cmra.com/risk_standards_working_group.php).

Citing that publication in 2008, the BSRMF noted that such prior work compilations included institutional, hedge fund and banking perspectives. It saw the need to specifically address *"traditional asset management firms in developing and assessing their risk management programs."*

Meanwhile, there have been numerous regulatory pronouncements and actions of relevance to the buy side. Preceding the global financial crisis, in 2004, the Organization for Economic Cooperation and Development produced a discussion draft, *"Governance of Collective Investment Schemes,"* (http://www.oecd.org/finance/financial-markets/33621909.pdf), which was an iteration of a previous statement of principles by the International Organization of Securities Commissions (IOSCO).

The U.S. Dodd-Frank Act of 2010 and, on varying timetables, the Basel III and Solvency II capital rules and the European Union's Alternative Investment Fund Managers Directive, European Market Infrastructure Regulation and Markets in Financial Instruments Directive all had some, often major, impacts on buy-side firms and their affiliates.

IOSCO, on which virtually every securities market regulatory jurisdiction is represented, stepped up the pace post-2008, working through its Technical Committee's Standing Committee on Investment Management, and initiating consultation processes and principles touching both directly and indirectly on the buy side.

The July 2009 *"Good Practices in Relation to Investment Managers' Due Diligence When Investing in Structured Finance Instruments called attention to valuation issues affecting all firms trading in over-the-counter instruments: "*as a matter of internal control, registered intermediaries and investment advisers avail themselves of practitioners who are skilled or trained enough to model fair valuation adequately in illiquid market conditions." (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD300.pdf).

Subsequent IOSCO publications, indicating increasing global awareness of buy-side risk issues, included "Principles of Liquidity Risk Management for Collective Investment Schemes".

(https://www.iosco.org/library/pubdocs/pdf/IOSCOPD378.pdf) (April 2012); *"Principles for the Valuation of Collective Investment Schemes"* (http://www.iosco.org/library/pubdocs/pdf/IOSCOPD413.pdf) (May 2013); and a consultation on asset custody principles (http://www.iosco.org/library/pubdocs/pdf/IOSCOPD454.pdf) (October 2014).

1.2

The Enterprise-wide and Systemic Dimension

While risk management is well established on the buy side, the nature and complexity of the risks are ever changing. Many firms have responded by establishing enterprise risk management functions, typically overseen by chief risk officers. An enterprise-wide view, aided and enhanced by a new generation of data aggregation and analytical technologies, enables a holistic perspective and timely responsiveness on all risks affecting a business or organization.

Any given firm will define its spectrum of risks differently, based on its product and client mix, strategic profile, and where it does business. But every firm today finds its identified exposures increasing — and they are increasingly interconnected. For example, market and credit risks converge when a stock-price crash affects the creditworthiness of a counterparty. A natural disaster in one part of the world can disrupt currency markets, supply chains and entire economies far afield — spreading market, operational, vendor and liquidity challenges. A cybersecurity breach can be as much a reputational as it is a financial or operational event.

At the same time, the financial world is increasingly interconnected and interdependent, and regulators and central bankers are on alert as never before for risks that may have systemic consequences and the potential for contagion. The question of how "systemic" asset managers may be is a subject of lively policy debate. A 2013 paper by the U.S. Treasury's Office of Financial Research (http://financialresearch.gov/reports/files/ofr_asset_management_and_financial_stability.pdf) deemed "reaching for yield," among other asset-management behaviors, a potential threat to financial stability. That prompted critics such as Paul Schott Stevens of the Investment Company Institute to argue that in the financial crisis *"asset managers were not a source of risk, nor are they likely to be."* (http://www.ici.org/viewpoints/view_14_assetmgr_sifi).

Few if any buyside firms ultimately face the likelihood that they will be designated *"systemically important financial institutions"* and subject to tighter regulation than their peers. However, the fact that they are in the SIFI conversation is an indication of the critical roles they play in the financial world and the importance of risk management to their operations and performance.

The purpose of the principles set forth below is to provide a general framework reflecting that growing importance and understanding of risk from the buyside perspective. It is hoped that the principles will provide a useful reference for each any firm in developing and assessing its own risk management structures and programs.

2 Best Practice Risk Principles For Asset Managers

Risk Management Principles: A Framework

The following principles address issues that are typically relevant to buyside firms. For ease of reference, they are divided into three sections:

- The Governance section contains risk principles relating to organizational structure and oversight mechanisms. It addresses the importance of independent controls, segregation of functions, senior management involvement in risk management and oversight and adoption of appropriate policies and procedures.
- The Investment Risk section contains risk principles relating to the need for various risk controls at the portfolio level. It addresses market risk, liquidity risk, leverage, valuations and other aspects of investment risk.
- The Operational Risk section contains risk principles relating to various types of risks that occur in the ordinary course of business and in disasters. It addresses the importance of identifying, assessing, and monitoring these risks, putting in place adequate systems and minimizing manual processes, managing counterparty credit risk, and assuring business continuity in a disaster.

These principles are offered as a guide to boards, trustees, senior managers and risk personnel who are developing and evaluating their risk management structure. The degree to which any particular principles critical to any particular firm, however, will, as explained above, depend on many factors, and each firm is advised to carefully consider its particular risks and the most effective way to address them.

Governance Principles

- A robust risk management framework is essential to a common understanding of risks
- Segregation of functions provides a key organizational check and balance
- Clearly defined roles and responsibilities for managing risk are essential to effective governance
- Senior management's establishment of a risk conscious culture is a component of effective risk management
- An independent risk management group reporting and/or having access to the C-suite, CEO, and/or Board of Directors is a good check and balance
- Good governance includes transparent risk measurement and reporting
- Proprietary investment management has its own special risk governance considerations

Investment Risk Principles

- Client risk tolerances and expectations should be known, communicated, and monitored
- Investment risk should be estimated and monitored
- Investment performance should be measured and monitored
- Liquidity and capacity risk should be estimated and monitored
- Concentration risk needs to be tracked and understood
- Risks attributable to leverage should be tracked and understood
- Valuation methodologies should be fair and consistent
- Stress testing is an important tool in analyzing risk
- Issuer and counterparty credit risk should be estimated and managed

Operational Risk Principles

- Recording and reviewing internal and external operational risk events supports strengthening of the control environment on an ongoing basis
- Performing periodic risk and control assessments with business involvement is important to identify and prioritize risk mitigation activities
- Key Risk Indicators (KRIs) help to measure, monitor and report operational risks
- A forward-looking approach to operational risk quantification is important to support the quality of risk management decisions
- Coordination of the operational risk framework across control functions and adequate governance structures around the framework are critical to ensure its effectiveness

3 Governance Principles

Risk governance is the critical oversight of risk management activities within an organization, and involves the establishment of organizational decision-making structures (e.g. Committees) and issue escalation procedures. The key components of this oversight include:

- Senior management and board level understanding of risks, definition of risk tolerances, and setting of risk management and ethical tone
- Organizational checks and balances, including an appropriate segregations of duties.
- An organizational structure in which risk management roles and responsibilities are clearly defined. Risk governance should be supported by written policies and procedures
- Creating and maintaining a culture in which understanding and managing risk is everyone's responsibility
- Independent business groups, including a risk management function reporting and/or having access to the C-Suite, CEO, Board of Directors, and Executive Committee
- Risk management and reporting capabilities that inform decision-making

Although the form of risk governance will vary depending on the size and complexity of each organization, effective risk management generally requires focus on these governance elements.

3.1

A Robust Risk Management Framework Is Essential to a Common Understanding Of Risks

The term "risk" as it relates to asset management firms and assets under management has many nuances, and the methods of presenting the necessary metrics are numerous. The specifics and methodology of the framework are beyond the scope of this document. There must, however, be a common understanding and agreement by senior management of the firm's risk framework. This risk framework should among other things be incorporated into the metrics by which asset managers will be measured and likely compensated. Obviously the market environment is dynamic, and the most applicable metrics may change over time.

The framework — the construct which senior management has agreed to adopt — should be uniform cross-departmentally to provide the opportunity for risks to be assessed cross-functionally. Common and clearly defined terminology on risk management issues is essential for effective and clear communication and understanding.

3.2

Segregation Of Functions Provides a Key Organizational Check and Balance

Asset management companies must be organized in a manner that provides appropriate checks and balances. This involves the segregation of control functions from line functions (i.e. product development, sales, portfolio management and trading) as well as the segregation of functions to ensure independent verification of trade details, performance, valuations, etc. It is also important that there is an adequate segregation of investment and support functions. It is important that the person responsible for bringing in new clients and/or entering into transactions, i.e., the marketer, portfolio manager or trader, is not the person (or the subordinate or superior of the person) responsible for determining the acceptability of the client or counterparty from a credit perspective. Nor should marketers, portfolio managers, or traders be responsible for checking and entering full trade details, confirming, comparing and settling the trade, valuing the trade initially and on an ongoing basis, measuring performance and monitoring the risks attributable to the transaction (consistent with the risk measurement system that has been established), or determining whether it is acceptable to exceed established limits without participation of various control groups.

Appropriate segregation of functions requires that trades be verified, confirmed, compared, valued, etc. by people other than traders and that independent checks and balances exist at every stage of the process to deter intentional or unintentional misstatements and other errors.

3.3

Clearly Defined Roles and Responsibilities For Managing Risk Are Esstential to Effective Governance

3.3.1

Management and Staff Roles and Responsibilities

Effective governance requires that each person understand their roles and responsibilities with respect to risk identification and assessment, and mitigation within risk tolerances, as established by both internal and external stakeholders (e.g. clients). Common roles and associated responsibilities within a firm's risk governance structure include:

- **Boards of Directors**, trustees or other governing bodies have a responsibility to understand the major risks applicable to their firms and approve and periodically review the firm-wide risk management frame work, including how risk is to be identified, assessed, monitored and controlled.
- **Senior Management** is responsible for overseeing the establishment and implementation of a risk management framework, including policies, procedures, systems and methodologies, and for assuring they are complied with. Senior management must consider the risks attributable to new products and strategies before they are approved for first use and periodically thereafter. They should set risk tolerances at the enterprise level, monitor adherence, and receive information on an ongoing basis sufficient to enable the firm to anticipate problems and make midcourse corrections.
- **Line Managers** are responsible for complying with policies and procedures and should be evaluated on how well they do so.
- **Portfolio Managers** are responsible for maintaining levels of portfolio risk consistent with representations made to clients and/or required by client guidelines particularly with regard to risk tolerance and invest ment objectives.
- **Operations personnel** are responsible for adhering to operational policies and procedures to mitigate risk.
- **Control groups** such as legal, compliance, financial control and internal audit are responsible for measuring and monitoring risk and for conducting independent reviews of compliance with risk management and other policies.

3.3.2

Fiduciary Obligation Is Paramount

For buy-side firms acting in a fiduciary capacity, it is important that the nature and extent of their fiduciary duties be clearly understood by employees and clients alike. To accomplish this, fiduciary obligations should be clearly spelled out in applicable investment or management agreements and other legal documentation, and understood by all relevant parties. Equally important, employees need to be cognizant of their fiduciary obligations and to consider those obligations in their ongoing decision-making. If a particular action or decision would benefit one client or class of clients over another, or other conflicts of interest exist, such action, decision or conflict should be considered from a fiduciary risk perspective and appropriately disclosed and/or resolved. To the extent that a written ethics statement is in place, it should address how key conflicts are handled so as to minimize conflicts between the interests of multiple clients and the interests of the firm and its employees.

It is also important for fiduciaries to remember that placing client money with or outsourcing to external advisers and sub-advisers, administrators or other third-party service providers does not extinguish the fiduciary obligation owed to clients. Accordingly, it is advisable that third-party and outsourced relationships be reviewed and managed so as to assure that fiduciary issues are identified and fiduciary obligations are met.

The incorporation of a fiduciary mindset into a firm's culture is itself a risk "control." The implications of the responsibility buy-side firms hold, and the corresponding obligations as fiduciaries, simply cannot be understated and must exist within the firm's DNA.

3.3.3

Additional Resources For Risk Governance

Additional resources, such as written policies, ethics codes, guidelines, escalation procedures and similar documentation should be clear, unambiguous, accessible and achievable.

Asset managers and investment advisers are in many cases legally required to adopt written policies, procedures and ethics codes. Even where not legally required, written policies and procedures and formal ethics codes have become increasingly common for

asset management firms. These are useful risk management tools so long as they are realistic rather than aspirational and so long as they are actively communicated and followed. It is less risky to adopt policies and procedures that are realistic, even if flawed, than to adopt idealistic policies and procedures that cannot realistically be adhered to.

In addition to written policies and procedures, asset managers must adhere to investment guidelines provided by clients or disclosed in fund or account documentation. Because of the fiduciary and legal significance of staying within the relevant guidelines and disclosures, it is important that these documents be clear and unambiguous on their face, requiring little or no interpretation on the part of the firm. In addition to a legal review, guidelines and disclosures describing investment strategies, restrictions, etc. warrant careful review by affected business areas to be sure that each affected business unit has the ability to comply with such guidelines.

In a complex business environment, operational problems, limit breaches, etc. can and do happen and exceptions from established policies and procedures are occasionally necessary. In order to limit risks attributable to such exceptions, it is helpful to identify who within an organization has exception approval authority, how long various exceptions can exist, who in the management chain needs to be apprised of exceptions, and what documentation needs to be kept. It is also useful to determine in advance what exceptions, particularly those involving investment guidelines, should be brought to senior management and/or a client's attention, as well as the time frame within which to do so.

If and when errors occur, it is important to convert instances into a learning experience. Processes across operational groups can be similar. Thus, thoughtful "post-mortem" error analysis can often be effective and actionable for multiple groups, not just the group where the particular error occurred.

3.4

Senior Management's Establishment Of A Risk-Conscious Culture Is A Component Of Effective Risk Management

One of the most important risk controls a buyside business can have is a risk conscious culture in which risks are well understood, tolerances are clearly defined and risk/return tradeoffs are considered. Creating a risk-conscious culture requires conscious effort by senior management. In addition to determining and communicating their risk tolerances, senior managers set the ethical and fiduciary tone for the organization. Whether or not this necessitates the adoption of a formal ethics policy (as is legally required under some regulatory schemes) or a less formal but equally rigorous articulation of values, effective risk management involves having senior management define both the risk profile and values of the organization, communicate them to employees at the outset of the employment relationship and periodically thereafter, and require that those values be adhered to at all times by themselves and their employees.

Viewed in the broadest sense, risk management is the responsibility of all. Employees at every level must be cognizant of risks and willing to do their part to make sure those risks within their sphere of responsibility are managed in a manner that is consistent with the firm's policies, disclosures provided to clients as well as client guidelines. Even the most detailed and sophisticated risk management programs are unlikely to be effective in the absence of a risk-conscious culture.

Depending on the applicable regulatory framework, many asset managers have a legal obligation to provide ongoing education to their employees with respect to ethics and compliance issues. Even where education is not legally required, it is a critical aspect of developing a risk-conscious culture. Employees need to be aware of what it means to be a fiduciary; what legal, compliance, and risk management issues are relevant to particular departments and the firm; how the firm chooses to deal with them as well as to understand the particular business issues applicable to various functions; and how they may change over time. The better employees understand the risks attributable to their businesses, products and functions, the more likely they are to incorporate them into their decision-making.

3.5

Independence Of Risk Management From Investment Management, Trading, and Client Service Is a Good Check and Balance

Regardless of how they are structured, risk management groups need to have sufficient independence to be able to perform proper risk management. This generally means that they should report in a way that provides independence from the business lines whose risk they are charged with managing, and possibly have access to the board (directly or via access to executive sessions), the CEO or to other very senior levels to assure proper stature in the firm as well as access to key decision makers.

While a dedicated risk management staff may not be feasible or appropriate for all firms, a knowledgeable, skilled chief risk officer ("CRO") reporting and/or having access to the C-suite, Board of Directors, Executive Committee or the like can be an important component of effective risk management. Regardless of reporting lines, a mechanism by which the opinions of the risk manager can be freely communicated to senior management and the Board is a valuable component of effective risk management.

A broader, more proactive CRO role for consideration and analysis of risk can be beneficial. This might entail independent risk personnel considering risk on both an enterprise-wide and discrete basis, coordinating the periodic identification of risks by various business groups, as well as providing input into investment strategy, risk budgeting, portfolio construction, etc. on an advisory basis. It is useful to consider whether risk is being taken intelligently and strategically with a reasonable expectation of being rewarded. The goal is not to eliminate risk, but rather to identify and understand risks being taken and insure that the risks retained are well understood, well managed, and consistent with the client's mandate.

Another role of a CRO is to identify opportunities where risk can be laid off or transformed. Some firms, for example, are more skilled at managing market risk than operational risk and might elect to outsource complex, operational-intensive risk and take on direct market risk instead.

The CRO is also generally a key member of senior management and can add substantial value by briefing line managers on evolving practices and new tools as well as systemic risk themes as they evolve. The CRO should oversee the creation and implementation of written risk policies that are clear and realistic rather than aspirational. While line-of-business and control groups such as Legal and Compliance are involved in creation of policies, it is often the CRO who champions risk policies that are relevant to the firm, that are consistent and adopted throughout the organization, and that are followed and updated. One of the most important roles of effective risk policies is to ensure risk transparency by clearly identifying exceptions and establishing appropriate escalation procedures, and related documentation.

3.6

Good Governance Includes Transparent Risk Measurement and Reporting

Risk metrics and output can be disseminated in numerous ways. Even the most insightful and crucial information may get lost if it does not reach the appropriate stakeholders. The way of communicating risk metrics and output can be crucial for their efficient use. Each firm must determine the optimal method for risk materials to be delivered and disseminated and identify the right forum and communication methods so that the information becomes understandable or "actionable." It is incumbent on risk professionals to ensure that their conclusions are communicated and known in advance whenever possible. While "false positives" are possible, the benefits of ample communication flow are far more than the damages of not being communicated sufficiently and in a timely manner. It is also possible to act with some level of incomplete information in situations when time is of the essence. An effective risk manager makes no assumptions but communicates in an effective manner until there is mutual understanding or "transparency" within the firm. Certainly mutual agreement is not expected or required, but the risk manager's role as an objective observer includes effective communication to peers who may have different levels of experience in risk management. Risk management metrics and terminology need to be clear and illustrated if necessary.

3.7

Proprietary Investment Management Has Its Own Special Risk Governance Considerations

Buy-side firms have their own unique risks, which need to be reflected in oversight, both internally and in terms of regulatory view. In asset management, while managers predominantly focus on managing client assets, there are activities where the manager's own assets can be exposed to investment risk. Investment risk from proprietary activities affects the manager's own balance sheet, profit and loss, reputation, and possibly even viability. Examples of these activities include:

- **Seed capital.** Some managers provide capital to new investment products in order to build live — and later marketable — track records with real money. The manager then becomes exposed to the collective absolute investment risk of the seeded portfolios.

- **Co-investment.** Some managers may invest along with clients in managed portfolios or other invest ments such as physical real estate or private equity. While the nature of co-investment can vary widely, the underlying investments will typically offer lower liquidity than a typical seed capital holding.

- **Guarantees.** Certain investment products have guarantees such as principal protection, performance levels, and stable net asset values. Managers are typically compensated for these guarantees via higher fee levels.

Proprietary investment risk should generally be managed using the same investment risk principles articulated in this document — except that the manager is the "client." Special considerations for proprietary investment risk include:

- **Governance framework.** Firms should establish a governance structure that promotes transparency, accountability and oversight over the firm's proprietary investment risks while facilitating the objectives of the activity. Particular attention should be paid to avoiding conflicts between the manager's proprietary investment activities and investment activities on behalf of clients.[1]

- **Profit and loss allocation.** The manager should clearly define how P&L from proprietary activity is allocated within the firm. The incentives created from proprietary P&L should be properly aligned with the activity's objective.[2]

- **Risk/reward assessment.** Managers should assess the intended rewards of proprietary activity — for example, more business and increased fees. The intended rewards might not explicitly include investment gains, causing the manager to evaluate the investment risk differently than if it were incurred by an external client's portfolio.

- **Hedging.** Some proprietary investment risk exposures can be hedged. Managers should consider the purpose of the activity when assessing hedging programs.

4 Investment Risk Principles

Asset and wealth managers (hereafter "managers") are fiduciaries investing funds that belong to their clients. Accordingly, the investment guidelines and risk tolerances that guide the manager's behavior must be targeted to the best interests of the client.

Investment risk is lack of certainty about future behaviors of portfolios. This uncertainty about the future encompasses both positive and negative outcomes. Accordingly, investment risk management is different from hazard management; the latter only contemplates avoiding or mitigating the consequences of undesired outcomes. Investment risk management seeks to understand and to shape the distribution of future portfolio returns (1) to allow for desired positive results; while (2) keeping the probability or impact of negative results within desired ranges.

4.1

Client Risk Tolerances and Expectations Should Be Known, Communicated, and Monitored

Managers should understand the risk tolerance and return expectation for each portfolio they manage. Specifications of risk tolerances and expectations for the behavior of client portfolios may originate with the client or with the manager. In some cases quantitative measures may be appropriate; in others qualitative descriptions will be used; and in others there will be a combination of quantitative and qualitative specifications of risk tolerances and client expectations.

When a portfolio is separately managed for a single client, the manager should discuss risk tolerances with the client. When a portfolio is a pooled vehicle, methods to determine risk tolerances may vary depending on legal jurisdiction and type of vehicle, but they could include: communication with the vehicle's board of directors or trustees; use of documents such as prospectuses; and determining the risk patterns of peer groups.

Within the bounds of applicable regulation, managers should clearly communicate the expected risk patterns of an investment vehicle, and should ascertain whether or not they have the capacity to properly estimate the relevant risk characteristics before they agree to do so.[3] Risk tolerances and return expectations may change over time, so managers should regularly reassess whether or not they are current.

Managers are often required to focus on the uncertainty of future portfolio behaviors relative to a benchmark.[4] In this case, the uncertainty of the benchmark's behavior is not the responsibility of the manager, but the manager is responsible for managing the variability of returns relative to the benchmark. In other cases, the variability of total returns is of interest; this is equivalent

to setting a benchmark equal to zero. Whether risk is benchmark-relative or absolute, the metrics that quantify risk vary by client. Popular metrics include, among many others: tracking error; expected shortfall; value at risk (VaR);[5] expected drawdowns under certain stress scenarios; and maximum drawdowns under historical simulation.

Whatever tolerances and expectations are targeted, managers should determine whether lower bounds are as important as upper bounds. Some clients may feel that their managers will not be able to produce a targeted level of return if they don't take enough risk and will be just as concerned about too little risk as they are about too much. Other clients will want to leave lower bound decisions to the discretion of their manager. For separately managed accounts where direct discussion with the client is feasible, managers should discuss this issue. For other accounts, the manager should communicate its approach.

Clear procedures should be put in place for dealing with portfolios that are crossing risk tolerance levels. These might include: escalating discussions with clients, senior management, and others as parameters warrant; hard or soft limits; and hedging techniques.

Just as portfolio managers generally make it clear that they cannot promise a given level of return in a risky portfolio, so too should they avoid promising a specific outcome with regard to a given risk statistic. Given reasonable cure periods to react to market movements, when appropriate a manager can endeavor to keep ex-ante risk estimates at certain levels. However, it is necessary to have clear client communication about the fact that — despite best efforts to manage risk — ex-post risk measures can vary from the desired outcome.

4.2

Investment Risk Should Be Estimated And Monitored

Once the appropriate metrics and levels to capture investment risk tolerances have been selected, these metrics should be estimated and monitored regularly.

Because risk metrics attempt to describe the distribution of future investment returns, they endeavor to be forward-looking quantities that are estimated rather than backward-looking quantities that are precisely measured. Ex-post risk metrics may be computed to provide context and validation of ex-ante estimation methods, but managers should understand and communicate that ex-post risk metrics are not necessarily the best predictors of future risk behavior.

No one statistic suffices to describe complex investment risk in its entirety. Each metric has its strengths and weaknesses. For example, 99% VaR is silent on what could happen in the 1% of cases beyond its horizon. A risk manager looking at a single metric can get a distorted picture of risk by focusing on a single risk element. It therefore is advisable for managers to avoid over-reliance on any single statistic. They should instead use a variety of statistics that quantify different aspects of investment risk.

Managers should periodically assess whether or not their ex-ante estimates of risk metrics are providing reasonable predictions of subsequent behaviors. For example, a manager may want to check that 1-day, 99% VaR estimates actually encompass close to 99 out of 100 of the portfolio's returns the day after the estimate is made. When the manager uses third party risk software, the manager should discuss with the vendor the validation techniques the product uses, and determine whether or not they are reasonable.

When practical, risk attribution should be performed in a manner consistent with the methodology used for performance attribution as described in section 4.3.

4.3

Investment Performance Should Be Measured and Monitored

Performance analysis is an important facet of investment risk management. Every portfolio should have a defined benchmark or other objective and should be monitored against that benchmark or objective. Managers should analyze "what happened" — the rate of return of a portfolio versus its objective; and "why it happened" — the components of portfolio construction that led to the observed behavior. The latter analysis is usually called performance attribution.

Performance attribution can be useful in determining whether or not the asset management process is working as expected. It can also be useful in determining whether risk models are identifying the key factors that drive portfolio behaviors. Some firms may find it useful to use more than one performance attribution method, possibly revealing unexpected performance and risk factors.

4.4

Liquidity and Capacity Risk Should Be Estimated and Monitored

Liquidity risk is uncertainty about future liquidity cost, in particular uncertainty about the cost of transacting in a timely manner in order to update a portfolio to reflect changing views of markets and securities; to meet funding obligations such as withdrawals from an investment vehicle; or to meet collateral calls. Security transactions incur costs based on the size, general market conditions, and urgency of the transaction. These costs — including fees, taxes, and movement away from the desired price — together constitute liquidity costs.

Managers should understand liquidity risk in their portfolios. Estimates of liquidity risk should encompass both normal and disrupted markets. The latter can vary radically from behavior during calm markets. In sufficiently disrupted markets, there may be no transactions possible.

Capacity risk is a form of liquidity risk. Products that may have no problems transacting in small volume can have very different behaviors as volume increases. When designing and managing investment products, managers should regularly assess the product's ability to obtain and provide appropriate liquidity and should limit the product's size if necessary. It is important to keep capacity issues in mind in marketing products and strategies and to equitably share limited opportunities with existing investors. Separately managed and collective investment vehicles may have different capacity criteria, as separately managed vehicles may have more flexibility as to when they demand liquidity.

The following elements should be taken into account to manage liquidity and capacity risk:

4.4.1

Liquidity Demand

Investment products should be designed and managed so that demand for liquidity incurred by investor subscription and redemption rights and patterns is aligned with the liquidity profile of the investments made by the product. Liquidity demand is also incurred by managers making transactions in order to react to changing market conditions. Counterparties can also be potential sources of liquidity demands — for example, for derivatives margining. Along with credit considerations described in section 4.9 below, managers should include liquidity considerations in their management of counterparty exposures.

Liquidity risks of investment products should be disclosed both to clients of separately managed accounts and to clients of pooled investment vehicles. Managers should consider both their ability to put cash inflows to work efficiently and their ability to meet cash outflow (redemption) requests. When they are managing a pooled vehicle, managers should assess the ability to meet redemption requests in a way that is fair to both redeeming and remaining clients. Useful indicators of potential liquidity demand include but are not limited to: investor base concentrations; portfolio flow volatility measures; and the general volatility of the market segment or segments in which the portfolio is invested. Investment firms offering multiple products that hold similar securities may also need to consider demands from internal funds competing for liquidity within the firm.

4.4.2

Liquidity Supply

Managers should consider the breadth and depth of the market segment or segments in which a portfolio invests. Potential investment types should be evaluated in terms of the time and cost expected for building up positions and for liquidating them. Portfolios should have appropriate mixes of investments depending on liquidity demand, ranging from cash and cash equivalents to longer-term and less liquid investments. Useful metrics in assessing liquidity supply include but are not limited to: percentage of total security issuance held; percentage of median daily trading volume; bid/offer spreads; repo haircuts for similar securities; and volatility.

In addition to liquidity supplied directly by instruments in a portfolio, alternative sources of liquidity supply should be investigated as appropriate. These include lines of credit, repo financing, and inter-fund lending. Both the costs and the benefits of these sources of liquidity should be taken into account.

4.4.3

Liquidity Options

Managers should understand and manage other liquidity options such as: delayed or suspended redemptions; payment in kind; side pockets; liquidity fees; and swing pricing. Available liquidity options vary by legal jurisdiction.

Liquidity demands and market liquidity can change without notice and in unexpected ways. While product design and ongoing transparency and management of liquidity risk are crucial in preparation for a liquidity crisis, a key part of an effective liquidity risk management program is being able to respond quickly and effectively during times of stress. Liquidity crisis contingency planning and testing should be a part of liquidity risk management. While past liquidity crises can provide guidance as to possible stressed behavior, managers should also assess current market structure and its possible effects on liquidity under stress.

4.5

Concentration Risk Needs to Be Tracked and Understood

Concentration risk can affect a portfolio in several ways. A concentrated, undiversified portfolio has unique risks inherent to its structure. The impact of idiosyncratic risk of single exposures is lowered at the portfolio level when those exposures are reasonably sized, but large concentrations can weaken the beneficial effects of diversification. Concentration metrics include, but are not limited to: percentage of a portfolio held in a single issuer or ultimate obligor; percentage of a portfolio held in a similar group of securities; and percentage of a portfolio's key risk metric — tracking error, expected shortfall, maximum expected drawdown, etc. — accounted for by a single issuer or group of similar issuers.

In addition, large concentrations in individual instruments can make liquidation at mark-to-market prices difficult if those mark-to-market prices are based on typical transaction size and do not reflect the size of the position. As a result, mark-to-market values can differ significantly from liquidation values.

Managers should consider the concentration criteria that are appropriate for each portfolio: for example, it may be better to have a small number of relatively concentrated low-risk exposures than a larger number of riskier exposures. Once appropriate levels are determined, managers should regularly assess concentration risks in the portfolios they manage.

In addition to concentration risk at the portfolio level, management firms face concentration risk across portfolios with respect to both individual investments and strategies. Excessive concentrations across portfolios and excessive exposure to particular factors (for example, value vs. growth or collateral geography) have the potential to put a firm's franchise at risk and need to be tracked and understood. It is important to note that fiduciary duty to a manager's clients preempts the firm's duty to its franchise/shareholders, so actions to address firm-wide concentration issues should be taken only if they do not conflict with the best interests of the firm's clients.

4.6

Risks Attributable to Leverage Should Be Tracked and Understood

Leverage can be defined in a variety of ways. One common definition of portfolio leverage decomposes every instrument into its effective notional long and short components. The total value of the longs plus the total value of the shorts in the portfolio is then divided by the portfolio's net asset value to compute leverage. However, complexities can arise, for example, when assessing the effects of derivatives and structured products.

In view of the many possible meanings of leverage, it is important for a manager to have a clear, reasonable, and consistent definition of the term. For example, suppose a portfolio incurs a currency exposure via a foreign equity holding and hedges away the currency risk with a currency forward. The manager should be clear about whether the currency forward in this situation is to be considered risk reduction or leverage. Where practical, such definitions should be communicated to clients.

No matter how leverage is defined, it is important from a risk management perspective that the risks to a portfolio attributable to leverage be understood, tracked and managed.

4.7

Valuation Methodologies Should Be Fair and Consistent

Valuation risk is a subcomponent of investment risk that is particularly important for managers of collective investment vehicles, because inaccurate valuations potentially cause unfair treatment to one set of investors versus another. Investors who buy in at inflated prices or redeem at deflated prices might be unfairly disadvantaged.

For separately managed accounts, incorrect valuations can hide problems; can cause incorrect investment decisions to be made; and might inflate manager incentive compensation.

Fair and accurate valuations are essential, but reasonable people can differ widely on how complex or thinly traded instruments are valued. Accounting and disclosure requirements have heightened awareness and scrutiny of these issues. It is important to ensure that the valuation methods used to price instruments traded are not only fair but also consistent with best practices as well as all applicable laws, regulations and accounting standards. Valuation methodologies should be consistently applied and verifiable. Special procedures may be necessary for firms operating across time zones and portfolios with geographic diversification, as markets may not be synchronous.

In order to achieve fairness and consistency, managers often use a variety of objective third-party sources to price instruments in client portfolios. These sources include (1) market quotations if readily available and (2) various independent pricing and database services. In the absence of such sources, valuations may be determined by using pricing models based on verified assumptions, or other techniques. Otherwise, securities and assets in a client's portfolio are valued at "fair value"[6] as determined in good faith by designated decision makers within the organization.

A valuation committee can provide important supervisory oversight of the firm's procedures for valuing portfolio instruments. A valuation committee is often responsible for (1) approving overrides of prices, (2) determining what valuation methodology is appropriate in the case of securities for which there are no readily available market quotations, or for which special circumstances[7] make the use of readily available market quotations inappropriate, (3) approving models and the assumptions to be used in connection therewith, and (4) determining fair value for securities for which none of the methods set forth above is deemed to be appropriate.

4.8

Stress Testing Is an Important Tool in Analyzing Risk

Risk metrics that rely on assumptions about the distribution of future portfolio returns can suffer from the well-known tendency of capital markets to deliver surprising regime changes. A variety of techniques help to develop a combined quantitative and qualitative assessment of possible surprise regime changes:

- **Stress testing,** where a single risk factor or a small number of risk factors are given extraordinary shocks; the likely behavior of a portfolio (often versus a benchmark) is then assessed conditional on the shock. For example, an instantaneous jump of 100 basis points in the US Treasury 10-year rate is a common stress test for fixed income portfolios.

- **Historical scenario analysis,** where the behaviors of a number of risk factors during a past economic environment — usually an extreme one such as the 2007-2009 global financial crisis; the 2000 technology bubble; or the 1987 stock market crash — are applied to the current portfolio. Scenario analyses can involve an instantaneous move from the current levels of risk factors to the levels of those factors in the historical environment; or they can involve the change in risk factors over a past interval applied to the current levels. Managers should understand and communicate the fact that history does not repeat itself, but the behaviors of current portfolios under historical scenarios can still be revealing about how they might behave in the future.

- **Hypothetical scenario analysis,** in which a qualitative narrative about a possible future economic scenario is translated into the behaviors of specific market risk factors, which are then applied to a current portfolio.

4.9

Issuer and Counterparty Credit Risk Should Be Estimated and Managed

There are two types of credit risk that are relevant to managers:

- **Issuer credit risk** is the risk arising from the possibility of default on securities that specifically constitute borrowing by the issuer. The manager expects this risk to be a source of reward.

- **Counterparty credit risk** is the risk arising from the possibility of default on an instrument or transaction that does not constitute borrowing by the issuer. For example, consider a bilateral foreign exchange (FX) forward transaction in which party A agrees to buy 2 units of currency X in exchange for 1 unit of currency Y from party B at some specified future time. If currency X appreciates so that party B owes money to party A, then party A has counterparty credit exposure to party B. Counterparty risk does not directly lead to an associated expectation of reward. For example, in the FX forward transaction, party A's compensation is the potential profit if

currency X appreciates; the risk to the currency profit is a hazard that is incidental to, but inseparable from, the FX forward transaction.

Managers should assess and manage both issuer and counterparty credit risk in each of their client's portfolios. Managers may also want to assess aggregate counterparty credit risk across all the portfolios they manage in order to maintain flexibility to change exposures when the manager's credit opinions change.

Managers should also analyze and manage settlement risk – the uncertainty over whether or not an agreed transaction will take place. Most transactions involve DvP (Delivery versus Payment) mechanisms, where the failure of a party in the transaction can lead to unexpected cancellation of the transaction. Settlement failure does not involve the unmatched transfer of either party's cash or securities to the other party; rather, it involves the cancellation of a transaction that was thought to have occurred. Instruments with long settlement periods, such as leveraged loans, are particularly exposed to settlement risk.

A counterparty is an entity to whose counterparty credit risk a managed portfolio is exposed. Management of counterparty risk should include the following four elements:

4.9.1

Selection of Appropriately Creditworthy Counterparties

Managers should assess the creditworthiness of counterparties using the same techniques they use to assess the creditworthiness of issuers of debt securities, keeping in mind the different risk/reward profiles for bearing counterparty risk versus direct credit risk. In many regulatory jurisdictions, managers are encouraged not to rely solely on credit rating agencies for such assessments. In addition to credit rating agencies, some managers may choose to use internally generated fundamental credit analyses or internal or vendor quantitative models. Market-based measures such as the level of credit default swap spreads on the counterparty's debt[8] may be used when markets are deep enough to give meaningful spread levels.

4.9.2

Estimation and Limitation Of Net Credit Exposure

Managers should regularly calculate or estimate counterparty exposures to each counterparty in each portfolio that they manage. There are a variety of counterparty exposure metrics, including current exposure "(CE)", estimated exposure "(EE)", and potential future exposure "(PFE)". Managers who have maximum issuer exposure limitations (whether through investment guidelines or internal policies) should take into account both direct credit exposures (e.g. from stocks or bonds owned in a portfolio) and counterparty credit exposures. Concentration risk principles (see section 4.5 above) should be applied to the combined direct credit and counterparty credit exposures.

4.9.3

The Use Of Documents and Mechanisms That Determine Actions In Cases Of Default

Bilateral, non cleared derivative transactions should take place under generally accepted mechanisms such as an International Swaps and Derivatives Association "(ISDA)" contract, which specifies, among other things, actions to take in events of default, and the rules surrounding the provision of collateral. Managers should also be aware of the risks to which collateral is exposed, including appropriation.[9] When practical, managers should consider tri-party counterparty collateral arrangements at a custodial bank.

More heavily traded instruments may trade through central clearinghouses or exchanges. Managers should be aware of the credit waterfalls and mutualization procedures that such venues employ.

4.9.4

The Use Of Collateral and Appropriate Thresholds For Adjusting Collateral

Managers should take into account and (where possible) negotiate appropriate collateral exchange procedures to offset counterparty credit exposures. Collateral quality and price variability should be assessed so that the manager understands the likelihood of collateral covering part or all of the counterparty credit exposure in the likely stressed situation in which it is needed. In addition to the manager's own evaluation, market practice for collateral exchange[10] should also be taken into account.
Managers should also evaluate the appropriate thresholds for exchanging collateral — whether they are triggered by a transfer amount, a time period, or both.

5 Operational Risk Principles

Operational risk management is an important aspect of an Asset Manager's risk management program as it covers a broad range of risk types, which individually or in aggregation have the potential to impact the execution of the business strategy if not managed appropriately. The Basel Committee defines operational risk to be as broad as "the risk of loss resulting from inadequate or failed business processes, people and systems or from external events." Asset management firms should consider incorporating any unintended outcomes (not just financial loss) and all types of technology (not just systems) processes into its operational risk management approach.

The level of complexity of an Asset Manager's operational and technology environment affects its operational risk, so a firm should assess its overall risk profile to determine its risk management needs. The risk profile should be monitored regularly as operational risks can change rapidly. For example, the rapid evolution of technology and high pace of regulatory change both could quickly escalate a firm's risk profile if not managed properly. Outsourcing of services should also be closely monitored in order to ensure that changes in their operational/technology environments do not increase a firm's risks. While the Operational Risk Framework should be proportionate to the complexity of the organization, it should generally include the following components to be successful at keeping track of and managing the company's operational risk profile — all components are discussed in more detail in the sections below:

Operational Risk Framework
- Recording of Operational Risk Events
- Risk and Control Assessments
- Key Risk Indicators (KRIs)
- Operational Risk Quantification

For an Asset Manager to understand its risk profile, it needs to understand the types of operational risks that can occur, their likelihood and potential impact. Below is a high level list of operational risk types that can be considered in developing an Operational Risk Universe. More detailed risk descriptions are available in the Section 5.6. This is not intended to be an exhaustive list but a broad generalization of common risks.

Operational Risk Types
- Execution, Process and Delivery Risks
- Outsourcing / Service Provider Risk
- Financial Reporting Risk
- Legal and Regulatory Compliance, including Regulatory Change Risk
- IT / Technology Risk, including Information Security and Cyber Risks
- Human Capital Risk
- Business Resiliency Risk
- Fraud and Financial Crime Risk

5.1

Recording and Reviewing Internal and External Operational Risk Events Supports Strengthening of the Control Environment on an Ongoing Basis

A sound practice to consider within an Operational Risk Framework is to record Operational Risk Events, independent of the financial outcome of those events. This should include events that occur within outsourced operations as well as any sub-advisory relationships. An event might result in a financial loss, gain or no financial impact (i.e., near miss). While gains and near misses do not have a negative impact on earnings or asset positions, they can often be seen as an indicator for loss potential that requires risk mitigation activity. There are multiple benefits in developing a risk event database or process: 1) the ability to assess issues to determine root cause and look for trends; 2) improve client experience; 3) provide timely and consistent information reporting to management; and 4) reduce the firm's risk profile through remediation actions and/or the improvement of internal controls. Another sound practice to consider is analyzing risk events of other firms and industries to understand the scenarios and assess if similar incidents could occur to your firm. When implementing a risk event reporting process, strong consideration should be given to: 1) using standardized and/or centralized reporting to better enable analysis of root cause and trends and to consolidate management reporting; 2) avoid, if practical, imposing dollar thresholds on the events to be recorded; and 3) reporting both financial and non-financial events (e.g., client reporting errors, compliance violations). By incorporating all of the above, there is increased consistency in management reporting and all operational risk events can be reviewed collectively to gain knowledge and potentially avoid future, more impactful events. Findings from root cause analysis, particularly for discovered emerging trends, should result in an appropriate risk remediation such as avoidance, reduction, sharing or acceptance, together with possible improvement in internal controls.
Centrally tracking operational risk events facilitates the ability to monitor the results of the risk response.

5.2

Performing Periodic Risk and Control Assessments With Business Involvement Is Important to Identify and Prioritize Risk Mitigation Activities

Firms should establish processes to identify, assess, monitor and mitigate known firm risks. This is accomplished by undertaking both a top-down and a bottom-up approach to identifying and prioritizing risk mitigation processes. It is important to engage senior leaders from relevant functional groups, compliance, product and technology areas to develop a top-down view of the critical topics and business areas that should be reviewed by risk groups. The top-down assessment provides the necessary information to prioritize the processes and products that should be analyzed through detailed, bottom-up assessments with process / product owners. During the planning phase, risk professionals should gather information regarding the systems and service providers (internal or external) that support the products and/or process. Complex business and system processes that traverse multiple business groups require risk professionals to develop a detailed end-to-end understanding of the process, underlying data and risks posed by key service providers.

The bottom-up risk assessment process can be implemented with the active participation of the process, system and product owners who inform the risk professionals regarding the effectiveness of the current internal control environment. The assessments are facilitated with business and technology groups who provide the procedures and related artifacts that deliver an operational view of the current process and associated controls. An important aspect in the process is a collaborative identification of the controls (including key controls), the review of the effectiveness of the controls, and any resulting observations for improvements to existing controls. It is helpful to drive accountability by identifying associates who will own the remediation of the impacted controls within a stipulated time frame. Additionally, monitoring the remediation of the identified actions is a relevant component of the operational risk program, which can be facilitated by timely risk reporting. The bottom-up assessment program should be flexible so that updates are made to the internal controls inventory as changes are made to products, process or the supporting technology / service provider infrastructure. The role of information technology is pervasive and critical to asset management as firms strive to support complex securities, alternative products, achieve scale and maintain a global presence. As a result, it is important to give due attention to relevant IT controls which include IT general controls and application controls.

Other related components that should be reviewed include information security, IT governance and disaster recovery to ensure the integrity, confidentiality and availability of key systems.

The aforementioned processes encapsulate the key steps required to conduct an assessment of the design effectiveness of the control environment. The next component in the risk and control assessment process is the evaluation of the operating effectiveness of the internal control environment, which is accomplished by testing key controls. Risk professionals should inform the impacted control owners at the outset of the testing program requirements (frequency, approach, sample requirements, etc.). Upon receipt of the testing data, the risk professionals should review it to establish whether controls are being implemented consistently and to further refine their operational understanding of the control environment. The control testing group also coordinates the timely reporting of testing results. Any testing-related observations should be researched, remediated and tracked as a component of the risk management program.

5.3

Key Risk Indicators Help to Measure, Monitor and Report Operational Risks

An important aspect of an effective operational risk management program is the ability to measure and monitor the effectiveness of key controls. This is typically accomplished by defining Key Risk Indicators "(KRI)" or measures associated with the key controls identified during the risk assessment process or for important processes within the asset manager's complex. Ideally, developing leading KRIs with good predictive capabilities are critical to the successful management of identified risk areas. KRIs include different types of metrics such as causal indicators that are aligned with root cause of risk events (e.g., system down time), volume indicators, and loss or near miss indicators.

The successful identification and implementation of effective KRIs requires the adoption of a structured approach. It starts with the risk assessment process during which risk professionals work with subject matter experts to evaluate the suitability and effectiveness of potential metrics as well as the identification of risk areas by senior managers and leaders of the firm. KRI information can be reviewed, monitored and escalated if it is measured against thresholds that have been defined in conjunction with control and process owners. Thresholds can be defined at different levels based on the risk management operating model adopted by the Asset Manager. It is essential to ensure that a controlled process exists to ensure that clear escalation criteria and protocols have been established when a KRI threshold is breached.

The next step is the development of dashboards for the aggregation and reporting of the various metrics for review by process owners, risk managers and senior management. Furthermore, risk groups should establish a review schedule to ensure that KRI information is reviewed and updated on a scheduled basis so that the metrics as well as the thresholds remain relevant and reflective of the operating environment. The review of KRI in conjunction with Operational Risk Event data should also inform the prioritization of risk assessment efforts.

Effective risk management is delivered by implementing processes designed and sustained by management to reduce the occurrence and impact of material risk events. This can be facilitated by the frequent measurement of the effectiveness of key processes, which is best enabled by standardization and good design.

5.4

A Forward-Looking Approach to Operational Risk Quantification Is Important to Support the Quality of (Risk) Management Decisions

The quantification of operational risk is important as it defines potential impact to the business and provides comparison with other risk categories. Quantification supports embedding risk culture into the company's management routines since it enables assessment as to whether risk exposures are within the company's established Risk Appetites and Risk Tolerances and to prioritize areas for risk mitigation.

Two prominent approaches to quantify operational risk are to use Operational Risk Event data or a scenario based approach. The method chosen should be proportionate to the size and complexity of an Asset Manager; companies may have a different focus for using data from events or scenarios (or other applicable methods). It should be understood that the quantification of operational risk (potentially, as of any other risk) cannot be exact and may only provide one potential version of the facts; however, finding a reasonable numerical assessment can support the quality of (risk) management decisions.

Each organization should be able to substantiate its choice of quantification method. This might be more challenging when relying purely on information of actual events, which occurred in the company (or to its competitors). Scarcity of event data may lessen its value for quantification and in the reliability of results as some events occur very rarely or not at all. Significant changes to the business model and/or environment can affect the ability to rely on prior events — examples include:

- The expansion of a single Asset Manager or the whole asset management industry into more complex investment products or new asset classes is accompanied by revised and new regulatory requirements, thereby changing the legal and regulatory risk profile of companies.

- The risk of loss of critical data assets (e.g., investment and/or customer data) through hacking attacks has increased significantly during the past few years. It is not foreseeable that the accelerated pace at which cybersecurity risk and related potential for information security losses to Asset Managers will reduce anytime soon.

- The increased level of outsourcing to third party service providers has changed not only their outsourcing risk profile but such significant changes to an organization's business model can lead to many process and control changes and could therefore increase the exposure in other (operational) risk areas (e.g., country risk and service provider oversight).

A scenario-based approach to Operational Risk Quantification overcomes most of the issues connected to historical data: it is forward looking, and considers the quality of existing controls. It can cover company activities, which are rarely represented in the internal and external event data, and it provides an up to date risk profile. The key challenge to a scenario-based approach is that it relies to a great extent on judgment to produce the risk profile. The key to success is the identification, assessment, challenge and validation of the scenarios through involvement of business experts, supporting factors and senior management sign-off. Clarity of understanding and business ownership of the chosen scenarios along with appropriate governance around the process help ensure its credibility.

5.5

Coordination of the Operational Risk Framework Across Control Functions and Adequate Governance Structures Around the Framework Are Critical to Ensure Its Effectiveness

Operational risk is the responsibility of every employee and requires an appropriate governance structure, accompanied by the right tone from the top. As part of an effective Operational Risk Framework, roles and responsibilities across control functions should be clearly defined.

The exact structure of the control functions varies across Asset Managers. In some companies the Busi-

ness Continuity Management "(BCM)" and IT Risk programs are driven by their Risk Management function, while in other firms IT is responsible. Some companies have a central Risk Management department, whereas other organizations operate a more decentralized approach with only a small Risk team and Operational Risk Managers in the business functions. Also, the allocation of risk-related responsibilities between the Risk Management and Legal and Compliance functions varies across Asset Managers. One common finding across organizations is that not just one function may own all components of the Operational Risk Framework and provides operational risk oversight.
In a situation where various control functions run their operational risk programs in an uncoordinated manner, the business may be approached multiple times for similar questions and senior management could receive risk reports, which overlap and / or provide conflicting messages. Therefore, it is important that control functions work together in defining and executing their components of the organization's overall Operational Risk Framework to prevent risk management fatigue of employees in the business, provide senior management with clear risk profile data, and ensure the effectiveness of the overall framework.

As an increasing number of firms operate in multiple locations, it is important to adopt a Governance, Risk and Compliance "(GRC)" system that to administer the firm's risk event, assessment and metrics information. A GRC system allows to store risk information centrally and to share it across the Three Lines of Defense.

5.6

A Sampling of Operational Risk Types

Below are a small sample of operational risk types that may be considered in developing an Operational Risk Universe:

- **Execution, Process and Delivery Risks**
  The risk arising from processes not delivering their products or services in the foreseen time or quality due to any reason, inclusive of unclear responsibilities and/or accountability due to ineffective corporate governance and set-up of the organization. Execution, Process and Delivery Risks contain the risk of loss from project failures due to the project or significant parts of the project not being completed or not being completed in time or the foreseen quality.

- **Outsourcing / Service Provider Risk**
  Any risk arising from service providers not providing contractually agreed services at all or not in the foreseen quality or time.

- **Financial Reporting Risk**
  The uncertainty or risk to the firm by failing to file accounting statements according to the appropriate accounting standards (e.g., US GAAP / IFRS) or with due care and attention with regard to the appropriate audit process.

- **Legal and Regulatory Compliance Risk, including Regulatory Change Risk**
  The risk of clients, employees or counterparties taking legal action against the firm resulting in protracted litigation, financial loss and reputational damage. The risk that the company fails to meet its regulatory requirements or fails to manage changes in regulatory requirements with respect to new legislation, resulting in investigations, fines or regulatory sanctions.

- **IT / Technology Risk, including Information Security and Cyber Risks**
  Any risk associated with the use, ownership, operation, involvement, influence and adoption of IT within the firm or its service providers. IT / Technology Risk consists of IT-related events that could potentially impact the business, inclusive illegal or unauthorized use of computer systems and data.

- **Human Capital Risk**
  Risk that the company may incur losses due to drain or loss of personnel, deterioration of morale, inadequate development of human resources, inappropriate working schedule, inappropriate working and safety environment, inequality or inequity in human resource management or discriminatory conduct.

- **Business Resiliency Risk**
  Potential impacts to the ongoing operation of the company resulting from natural disasters, man-made disruptions, inclusive terrorist attacks, and biological / geo-political events.

- **Fraud and Financial Crime Risk**
  Any risk of loss arising from employees or third parties acting in an inappropriate or dishonest manner resulting in a financial loss to the firm (e.g., funds stolen) and consequential damages to its reputation.

5 Footnotes

1. It should be noted that risk management oversight of proprietary investments likely falls under the jurisdiction of a corporate board of directors rather than a fund board of directors, which oversees risk for outside investors.

2. Some firms may assign a "cost of capital" to seed capital funds to encourage prudent use of these limited funds and to discourage extended use of funds for products not meeting expectations within a reasonable time frame.

3. The UK court case Unilever Superannuation Fund v. Mercury Asset Management plc is often cited as involving, among other things, ambiguous expectation setting. The case was settled privately during a 2001 trial.

4. Benchmarks are portfolios that are used for comparison and that satisfy the CFA Institute criteria: unambiguous; investable; measurable; appropriate; specified in advance; and owned. http://www.cfainstitute.org/learning/products/publications/rf/Pages/rf.v2011.n1.1.aspx?PageName=searchresults&ResultsPage=1, p. 6.

5. VaR is widely used in banks and other "sell side" firms and has become used in some buy side frameworks. However there is extensive literature discussing the "incoherent" nature of the value-at-risk measure; see for example Artzner, Delbaen, Eber & Heath, "Coherent Measures of Risk," Mathematical Finance, Vol. 9, No. 3 (July 1999), 203-228. The expected shortfall measure has been gaining regulatory favor for banking applications; see for example www.bis.org/publ/bcbs219.pdf and www.bis.org/publ/bcbs265.pdf.

6. Fair value procedures should be appropriate to the portfolio's jurisdiction. In the US, SFAS 157 is used. In many other jurisdictions, IFRS 13 applies.

7. "Special circumstances" might include ownership of a very large or illiquid position, or other factors that, in the reasonable judgment of the valuation committee, would likely make market quotations or the prices obtained from independent pricing and database services inadequate measures of the value of a position.

8. Consideration should be given to the type of debt whose credit default swap spreads are used to provide information about creditworthiness; this debt should be as close to pari passu as possible with the counterparty exposure being assessed.

9. For example, customer funds were appropriated by MF Global in the period leading up to its 2011 bankruptcy, although eventually most funds were returned.

10. See for example survey data at http://www.newyorkfed.org/banking/tpr_infr_reform.html and http://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/short-term-markets/Repo-Markets/repo/latest/

Creating a culture of
risk awareness®

Global Association of
Risk Professionals

111 Town Square Place
14th Floor
Jersey City, New Jersey 07310
U.S.A.
+1 201.719.7210

2nd Floor
Bengal Wing
9A Devonshire Square
London, EC2M 4YN
U.K.
+44 (0) 20 7397 9630

www.garp.org

About GARP | *GARP enables the risk community to make better informed risk decisions through creating a culture of risk awareness. We do this by educating and information at all levels, from those beginning their careers in risk, to those leading risk programs at the largest financial institutions across the globe, as well as, the regulators that govern them. www.garp.org*

GARP | Global Association of Risk Professionals