Exploring Evolving Risks and Challenges
Perspectives from the investment management industry

Based on the results from Deloitte’s Global Risk Management Survey, eighth edition
Introduction

Enough time has passed since the height of the financial downturn to provide us with an opportunity to look back and review not only how risk management practices have changed in its aftermath, but also how risk management needs to evolve further to address growing and emerging risk areas.

Not surprisingly, our survey findings indicate a heightened focus on governance and oversight, as well as increased attention in managing liquidity, investment, credit, regulatory, and reputational risks among others. However, the broader implication is that this necessary focus also resulted in a shift in management’s attention and resources away from other risk areas, particularly in the area of operational risk and some of the growing and evolving risks that the industry is faced with today.

Utilizing the eighth edition of Deloitte’s Global Risk Management Survey of financial services firms, we will explore these trends in the context of investment management. One-half of the 86 respondents identified themselves as either stand-alone investment managers or investment managers of larger integrated financial institutions (primarily banks and insurance firms).

The Global Risk Management Survey, eighth edition, assesses the state of risk management and confronts today’s challenges and evolving needs. The survey was conducted from September to December 2012: chief risk officers or their equivalents from 86 financial institutions from around the world, with aggregate assets of more than $18 trillion, participated.
Lessons learned: How risk management has evolved

**Governance and oversight**

The strategic importance of risk management and the potential for reputational harm can be seen in the 94 percent of respondents who indicated that their boards and/or executive management teams are spending more time on the oversight of risk compared to five years ago. Another key indication of the heightened focus on risk is the 80 percent who said their boards now review and approve their organization’s risk management policy and/or enterprise risk management (ERM) framework, as well as their risk appetite statement. In the context of private equity and hedge funds, risk committees or working groups are increasingly taking on a role similar to the responsibilities of a board in other firms.

We have also seen significant growth in the adoption of ERM programs. In this year’s survey, 62 percent of organizations reported having an ERM program in place, up from 52 percent in 2010 and 36 percent in 2008. An additional 21 percent of financial institutions indicated that they are actively building an ERM framework. To put that in context, firms that have built or are presently building an ERM framework total 83 percent, representing a significant shift in the number of firms that seek to view and manage risk more holistically, versus the minority of firms who had an ERM program in 2008.

When asked about their effectiveness at managing specific risk types, most institutions rated themselves as extremely or very effective in managing liquidity risk (85 percent), credit risk (83 percent), counterparty risk (83 percent), regulatory/compliance risk (74 percent), and market risk (72 percent). However, fewer than half of the firms (45 percent) gave themselves a high rating for operational risk management — strikingly similar and a little less than the 47 percent recorded in 2010. This finding underscores the inherent complexity of managing and measuring operational risk, and strongly suggests that there is still work to be done to improve in this area.

**Other survey highlights**

Other macro themes across the broader financial services landscape have emerged which are worth noting:

- **Risk management capabilities improve**: Almost three out of four risk managers rated their institution to be either extremely or very effective in risk management overall, an increase from 66 percent in 2010’s survey results.

- **Firms continue to invest in risk management**: Two-thirds of financial institutions (65 percent) reported an increase in spending on risk management and compliance, up from 55 percent in 2010. The majority of institutions participating in the survey (58 percent) plan to increase their risk management budgets over the next three years, with 17 percent anticipating annual increases of 25 percent or more.

- **Technology and data are a significant challenge**: Technology used to monitor and manage risk is a particular concern and, according to our findings, significant improvements in risk technology are needed. Less than 25 percent of institutions rate their technology systems as extremely or very effective while 40 percent of institutions are concerned about their capabilities in the management of risk data.

- **Opportunity for greater alignment of risk taking and compensation**: Progress in linking risk management with compensation has changed only incrementally since 2010’s survey results. Currently, 55 percent of institutions incorporate risk management into performance goals and compensation for senior management, which is little changed from 2010.

The strategic importance of risk management and the potential for reputational harm can be seen in the 94 percent of respondents who indicated that their boards and/or executive management teams are spending more time on the oversight of risk compared to five years ago.
In our experience, as more investment managers leverage model-driven trading strategies and have a greater reliance on valuation and risk models, they are grappling with a variety of questions including:

• Do our models execute as intended?
• How do we best monitor compliance with investment objectives?
• In the event of an issue, what do we disclose and when?
• How do we appropriately protect the intellectual capital associated with our model?

Beyond the significant risks of monetary loss, regulatory violations, and the potential loss of intellectual capital, some model-driven strategies can and have exposed investment managers to serious reputational harm. Investment managers took notice when the Securities and Exchange Commission (SEC) charged three AXA Rosenberg entities with securities fraud for concealing a significant error in the computer code of the quantitative investment model that they use to manage client assets. The error caused $217 million in investor losses that were repaid along with an additional $25 million in fines.

The challenge is that model risk — or the risk that an institution may experience adverse consequences from a decision or action based on using a model — can arise from a variety of sources, including inconsistent specification, application, and implementation of a model. This is not isolated to model-driven trading strategies, but also to quantitative models used for the purpose of valuation, trade allocation, and risk management. This broad array of inherent risks and the severity of potential consequences are likely key factors in survey participants’ low confidence in model risk management capabilities: of the 61 percent of our survey respondents who said model risk was now included in their ERM program coverage, only 50 percent believe they are effectively managing it.

Addressing emerging risk areas

In addition to reporting difficulty managing operational risk, many of our survey respondents acknowledged that their risk management approach needs to improve to more effectively address certain growing and emerging risks.

Of more than two dozen risk areas we asked survey respondents to rate their effectiveness in managing, three emerging risk areas — model risk, IT security risk, and business continuity — ranked near the bottom. In each case, only half of the participants judged their organizations as effectively managing those risks.

To address model risk, some of the areas where investment managers are focusing their attention are model governance, model validation, deployment and maintenance.

Governance
Within governance, they are assessing their oversight and monitoring practices, roles and responsibilities, policies and procedures, and overall control framework. In addition, when considering the complexity of the model and the potential for key-person risk or if a third party is involved, stringent documentation on how the model executes becomes paramount.

Model validation
This includes reviewing the theoretical design of the model, the data inputs/assumptions, and the output compared to the intended use and context of the overall model strategy. Firms are using ongoing monitoring to highlight divergences between actual and expected performance. Firms are also looking to independent examiners to validate and recalculate the models utilizing stress and back testing.

Deployment and maintenance
Many firms are enhancing the process and rigor around the model’s development life cycle. Primarily this is seen through change management controls and procedures, model integration into existing systems, processes and procedures, and architectural modifications required to support model deployment.

Cyber security and data privacy

Cyber threats continue to evolve in a number of different and discouraging ways. In the past, talented hackers worked alone or in small groups, often with limited access to resources and their aspirations were more often than not fame and notoriety rather than financial gain. Today’s threats are more calculated, targeting systems with personal and financial information, as well as intellectual property that can be monetized into huge sums on the black market. Attackers may operate with significant resources at their disposal (organized syndicates and potentially state-sponsored groups), taking advantage of both advances in technology that automate large-scale information collection and the vast amounts of data made available through the popularity of social media and other outlets. In addition, politically motivated attacks or hacktivism pose additional concerns for high-profile institutions and sectors as evidenced by recent denial of services attacks that successfully caused disruption to financial services institutions’ consumer-facing websites.

In previous times, it was a common understanding that many threats arose from insiders. A new reality that should cause investment managers to pay attention is that in 40 percent of breaches, attackers gained access through third-party systems.

This reinforces the need for investment managers to understand their extended enterprise and the control frameworks that service providers have in place to secure client and transaction data, as well as intellectual property.

Industry response: Our experience

One leading practice among investment managers is to better understand their potential exposure by conducting a cyber threat assessment. Such assessments typically entail six key steps:

1. Analyzing the organization’s Internet-facing systems
2. Identifying indications of existing system compromises
3. Assessing sensitive data across the organization and whether it is vulnerable to Internet access
4. Analyzing vulnerabilities tied to employees’ access to sensitive information
5. Identifying potential targeting by external cyber threat actors
6. Uncovering other unsecure practices, such as the use of unencrypted transactional websites

The investment management industry’s reliance upon service providers heightens the need to consider all six components above in the context of their extended enterprise, considering their provider’s resources, processes, and infrastructure as potential points of exposure.

---

Business continuity management (BCM)

BCM has been challenged in the past through a number of events, including technological, natural, and unfortunately, terrorist activities. The base assumption was that significant improvements were made, which is most likely accurate, but Superstorm Sandy brought BCM practices back into the spotlight for many financial services organizations. In the investment management sector, the effects of Superstorm Sandy could be seen in the quarter-end timing and the duration of the disruptions, which stressed many investment management firms’ ability to calculate net asset value, generate reporting, and satisfy client requirements. This is reflected in the survey where only 52 percent of the firms surveyed felt they were as effective as they could be in managing business continuity.

Industry response: Our experience

The regulators have taken notice as the SEC, the Commodity Futures Trading Commission, and the Financial Industry Regulatory Authority have issued a joint leading practice statement on business continuity and disaster recovery in response to Superstorm Sandy. Subsequently, the SEC also issued findings based on examinations of business continuity plans of selected advisors affected by “operational disruptions caused by weather-related events last year.” These reports highlighted some of the following areas:

• Scrutiny of vendors and rating them on their BCM preparedness
• Logistics such as communication plans and the need for alternative locations, particularly plans that take into account the possibility of a geographically widespread outage
• Regulatory compliance, particularly in being able to meet regulatory obligations and ensuring BCM plans are updated to include any regulatory changes
• Periodic review, testing, and training that is conducted at least annually

In our experience, in the aftermath of Superstorm Sandy, BCM and disaster recovery have become a topic for the risk committee, in some cases even being elevated to the board level. Many firms are reevaluating or adjusting their strategies for dealing with extended disruptions, as Superstorm Sandy provided a number of data points to gauge the actual effectiveness and employee response to existing plans. Given the recent regulatory notice, it is likely that there will be renewed focus on the controls, procedures, and service provider oversight associated with BCM.
We have discussed some of the emerging risks facing our industry, but our survey also highlights a variety of challenges and inhibitors to managing risk effectively that are specific to firms providing investment management services. These range from data and technology, resourcing, and service provider oversight. We have selected a few of these challenges to explore further.

Figure 1. How challenging are each of the following for the investment risk management function in your organization?

<table>
<thead>
<tr>
<th>Risk Management Challenges</th>
<th>Extremely/Very Challenging</th>
<th>Somewhat Challenging</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT applications and systems</td>
<td>23%</td>
<td>61%</td>
<td>84%</td>
</tr>
<tr>
<td>Data management and availability</td>
<td>35%</td>
<td>45%</td>
<td>80%</td>
</tr>
<tr>
<td>Resourcing</td>
<td>29%</td>
<td>42%</td>
<td>71%</td>
</tr>
<tr>
<td>Analytics and reporting</td>
<td>26%</td>
<td>45%</td>
<td>71%</td>
</tr>
<tr>
<td>Third party service provider oversight</td>
<td>23%</td>
<td>42%</td>
<td>65%</td>
</tr>
<tr>
<td>Risk governance</td>
<td>19%</td>
<td>45%</td>
<td>64%</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>29%</td>
<td>29%</td>
<td>58%</td>
</tr>
</tbody>
</table>
Challenge: Data and technology

As indicated in our introduction, one of the key findings in the survey is that the technology used to monitor and manage risk is a top priority and concern across the financial services industry, including investment managers. Investment management firms face significant system, infrastructure, and data challenges that occur for a variety of reasons, including the traditional silos encountered among functions, mergers and acquisitions, product development, and overall adaptation to changes in the marketplace. These challenges are compounded by the investment manager’s fund and account structures, and its reliance upon service providers for technology and data. Data quality and consistency can be particularly onerous as a result, as evidenced by the 79 percent of the respondents to the survey who indicated they were somewhat or extremely/very concerned about data quality and management. “Garbage in/garbage out” may be an old adage, but data quality is still clearly affecting organizations’ ability to assess, monitor, and mitigate risk.

An area of considerable focus across the financial services industry is reference data. For investment managers in particular, the financial downturn exposed both the challenge in determining counterparty risk and the importance of being able to look through transactions to consistently identify legal entities engaged in financial transactions. Post downturn, the G20 mandated the Financial Stability Board (FSB) to work on the long-standing industry need for a unique, global, and standard Legal Entity Identifier (LEI), in order to help assess systemic risk and aggregate risk at an entity level. The FSB, along with many industry participants, has defined the format for a standard LEI and a global, federated approach to distributing LEIs. Subsequent phases of the LEI implementation will include hierarchy data, which will provide additional information to calculate counterparty risk. Ultimately, adoption of LEI across the industry should greatly enhance counterparty risk management capabilities for investment managers, but costs will be significant as well: not only will reference data need to be mapped and transformed, but existing data stores, operational, accounting, and risk infrastructures will need enhancement to accommodate the LEI.

There are also increasing technology and data needs associated with investment compliance monitoring, the Foreign Account Tax Compliance Act, Form PF, and the Alternative Investment Fund Managers Directive, all affecting the investment management industry recently; therefore, it is not surprising to see more than three-quarters (78 percent) are concerned about their technology systems’ ability to adapt to regulatory requirements. These significant regulatory changes require coordinated cross-functional efforts between risk, compliance, and IT, and also externally with the service providers who often provide component pieces (e.g., data/technology) to meet these challenges. This can be further exacerbated for investment management firms that already have a global footprint and are subject to multiple regulators and jurisdictional requirements.

The irony is that while the survey indicates data and technology is a very significant challenge to effective risk management, it can also be its single largest enabler. A bitter pill too often hard to swallow is how to effectively gauge the ROI upfront in implementing a potentially large, complex, budget, and resource intensive technology initiative. This is versus the opportunity cost of not implementing initiatives that can yield more effective risk management, scalability to meet product and client demands, and increased capabilities globally. That stated, it appears many of the survey respondents have made up their minds in this regard as enhancing risk, data, infrastructure, and technology capabilities has become one of the main investment priorities for institutions.
**Industry response: Our experience**

To address deficiencies in infrastructure, a chief goal of the investments that firms are making is in improving the quality and consistency of risk data, with nearly half of those surveyed (46 percent) planning to make significant investments in this area over the next 12 months. In fact, data-driven investments have grown markedly in importance since 2010: risk data quality and management was ranked as a priority by 63 percent of respondents in this year’s survey, up from 48 percent, while enterprise-wide risk data warehouse development increased to 51 percent from 35 percent.

In our experience, timeliness, availability, and quality of reporting is not only of greater importance internally for decision-making processes by investment managers, larger and more sophisticated institutional investors or parent organizations are requesting that individual managers make data extracts available for consumption by their own risk processes and infrastructure. While data warehouses have been a focus area for some time, they have not proven to be a “silver bullet” to solving risk data quality issues. One of the biggest challenges to improving and maintaining data quality is making sure it is already “clean” and accurate when it is placed into the data warehouse. Even though the tools to catch errors on input, such as missing or inaccurate data fields, have been available for some time, many organizations did not institute the error detection processes or assign responsibility for data quality. As a result, data governance is emerging as an important focus area for investment managers to address this. The chief data officer is a position we see more often at investment managers, with the responsibility to implement the processes needed to improve overall data quality and integrate business user accountability for the integrity of that data.

Lastly, addressing data challenges is paving the way for more sophisticated risk analysis, monitoring, and reporting. Advancements in enhanced risk and scenario analysis capabilities, including wider product coverage, richer visualization, speed, and availability of data are key requirements driving technology investment to support risk management. Although real-time risk analytics and risk aggregation may be relevant or feasible only for a handful of managers with strategies that rely upon high volumes and algorithmic calculations, the technology advancements driving these capabilities can benefit a broader audience. For example, for investment managers with complex, structured products, technology, such as in-memory processing and grid computing, can create the difference between canned, T+1 risk data produced in an overnight batch versus flexible scenario analytics, rendered in visualizations that can be refreshed intraday, providing proactive support for the decision-making process.

These investments primarily seek to improve and enhance the abilities of the risk function among others, but also to allow risk professionals the opportunity to relinquish a burgeoning cottage industry in data management to focus on their core competency, which is managing risk.
Challenge: Resourcing

Doing more with less is a familiar prospect for most of those in our survey universe, and this task is more onerous today given the increasing intersection of risk and compliance due to regulatory demands and global operating models. This is placing a premium on resources with the right skills to manage day-to-day risk while accommodating growing and emerging risk areas. Indeed, 71 percent of the respondents indicated resourcing is a somewhat or extremely/very significant challenge.

Challenge: Service provider oversight

Financial firms face a variety of risks associated with their reliance on service providers, including a failure to perform against performance standards and contractual obligations, theft, or inadvertent release of client-identifying data, dissemination of intellectual property (such as on strategy or trades), and regulatory breaches (such as on anti-money laundering requirements) and counterparty risk.

Although most firms in our survey are satisfied with their service providers, some believe they face a significant risk of nonperformance and have, therefore, strengthened their vendor risk management program accordingly. Forty percent of firms believe they have high potential exposure to the risk of nonperformance by their custodian and 35 percent ascribe this risk to their administrator. In addition, 23 percent and 20 percent felt they had high exposure to potential nonperformance by their prime broker and transfer agent while only 13 percent felt they had high exposure to potential nonperformance by their distributor.

Industry response: Our experience

In the investment management industry, we are increasingly seeing a shift to risk-based resourcing — or the allocation of resources to key focus areas as a result of strategic risk assessments designed to maximize the impact and value to the firm. The growing use of formal risk assessments has empowered organizations to compare and contrast risk exposures across areas that were traditionally managed in siloes. As a result, resource allocation decisions that were historically determined by the loudest voice in the room or potential for revenue generation can now be made with a more holistic view of organizational exposure (where the risk lies) and the ability to realize the strategic goals of the organization. It has also illuminated skill-set gaps (industry based and competency) and allowed for informed hiring decisions to more effectively manage key risk areas. In short, it is leveling the playing field and allowing for better allocation of a firm’s most precious resource — people.

Industry response: Our experience

Some investment management firms are working to gain a more holistic view of their extended enterprise by evaluating and trying to better understand the risk profile for each service provider. In addition, they are establishing a service provider oversight framework that aligns with their overall risk profile and incorporates the following considerations:

- Level and frequency of oversight
- Design of controls
- Active versus latent monitoring
- Key risk indicators
- Adherence to service-level agreements and contract terms
- Use and reliance on third-party reports (e.g., SSAE 16, Financial Intermediary Controls and Compliance Assessment, “FICCA” reports)

A specific new challenge for many investment managers has been introduced by the growth of omnibus practices in the shareholder servicing model, as traditional distribution partners join the ranks of the service providers. This fragmentation of transfer agent services has driven some firms to expand their oversight programs to incorporate a diverse pool of providers that do not necessarily conform to standard contracting practices and supplier/buyer influence and leverage norms.
Investment managers, like many of their counterparts in the broader financial services industry, are working to identify the most efficient and effective ways to focus their time and effort on managing risks — those they have traditionally needed to address in the past and those that are growing in importance or rapidly emerging. When discussing risk with our investment management clients, a key question is emerging around managing risk in general — what is the most efficient and effective way to focus our time and effort on risk?

Increasingly, we are seeing firms taking an approach of characterizing their risk in three views, which correlate directly to the level of priority and focus of the board, executive management, and risk committees:

1. Franchise threatening: The 10–15 key risk areas that can threaten the reputation and operating ability of the firm
2. Regulatory imperative: Fulfillment of fiduciary, regulatory, and legal responsibilities
3. The control environment: All other risks where the residual risk is understood and reviewed on a periodic basis against limits and acceptable losses

For investment managers, this is not a race to the top or bottom, but rather to a place where market participants can feel comfortable about the risks they are taking and facing — so they can concentrate more on growing the business and generating superior returns. We hope the findings provided in the referenced survey report provide insight and clarity into how the industry is tackling risk management.

Final thoughts
In whatever manner a firm is addressing their risk, our survey results indicate that financial services firms have elevated the discipline of risk management further and are turning to technology and advanced data solutions to increase their effectiveness. It also indicates that there is still work to be done to both head off emerging risks and address challenges that are inhibiting traditional risk management approaches. Meanwhile, the more evolved risk managers are taking this time to examine the nuances of their firm’s risk culture by devising new and improved ways to measure risk taking throughout their organizations, and stress the need for greater organizational awareness and integration across risk, IT, operations, compliance, internal audit, and legal functions.
Contacts

Industry leadership
Cary Stier  
Vice Chairman  
U.S. Investment Management Leader  
Deloitte LLP  
+1 212 436 7371  
cstier@deloitte.com

April Lemay  
Investment Management  
Audit and Enterprise Risk Services Leader  
Deloitte & Touche LLP  
+1 617 437 2121  
alemay@deloitte.com

Authors
Garrett O’Brien  
Principal  
Deloitte & Touche LLP  
+1 212 436 5250  
gobrien@deloitte.com

Michael Quilatan  
Senior Manager  
Deloitte & Touche LLP  
+1 212 436 2230  
mquilatan@deloitte.com

Acknowledgements
We would also like to thank the following Deloitte professionals for their support and contribution to the report:

Sam Auxier  
Principal  
Deloitte & Touche LLP

Michael Chung  
Director  
Deloitte & Touche LLP

Michael Fay  
Principal  
Deloitte & Touche LLP

Edward Hida II  
Partner  
Deloitte & Touche LLP

Miguel Miranda  
Director  
Deloitte & Touche LLP

Timothy O’Sullivan  
Director  
Deloitte & Touche LLP

Alex Ravenel  
Manager  
Deloitte & Touche LLP

Adam Regelbrugge  
Partner  
Deloitte & Touche LLP

Daniel Soo  
Principal  
Deloitte & Touche LLP

Alexey Surkov  
Partner  
Deloitte & Touche LLP

Brendan Winkler  
Senior Manager  
Deloitte & Touche LLP

Steven Zaki  
Senior Manager  
Deloitte & Touche LLP

Michael Zwecher  
Director  
Deloitte & Touche LLP

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all of whom are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this publication, rendering professional advice or services. In addition, this publication contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by anyone who relies on this publication.

© 2013. For information, contact Deloitte Touche Tohmatsu Limited.