Exploring evolving risks and challenges

Perspectives from the investment management industry

Ed Hida
Global Leader
Risk & Capital Management,
Global Financial Services Industry
Deloitte

Garrett O'Brien
Principal
Audit & Enterprise
Deloitte

Mike Fay
Principal
Audit & Enterprise
Deloitte

Michael Quilatan
Senior Manager
Audit & Enterprise
Deloitte

Based on the results of Deloitte's Global Risk Management Survey, eighth edition

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.

Unsurprisingly, our survey findings indicate a heightened focus on governance and oversight, as well as a greater emphasis on managing liquidity, investment, credit, regulatory and reputational risks. However, the broader implication is that this necessary focus has also led to management shifting 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 faces today.

Through 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. 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 covers today's challenges and evolving needs. The survey was conducted from September to December 2012 with the participation of chief risk officers or their equivalents at 86 financial institutions from around the world that manage aggregate assets of more than US$18 trillion

As used in this survey report, 'Deloitte' means Deloitte Touche Tohmatsu Limited and its member firms.

Lessons learned: how risk management has evolved

Governance and oversight

The strategic importance of risk management and the potential for reputational harm were flagged by the 94% of respondents who stated 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 came from the 80% who said their boards now review and approve their organisation'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 programmes. In this year's survey, 62% of organisations reported having an ERM programme in place, up from 52% in 2010 and 36% in 2008. An additional 21% 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%, representing a significant shift in the number of firms that are seeking to view and manage risk more holistically, versus the minority of firms who had an ERM programme 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%), credit risk (83%), counterparty risk (83%), regulatory/ compliance risk (74%), and market risk (72%). However, fewer than half of the firms (45%) gave themselves a high rating for operational risk management —strikingly similar to the 47% recorded in 2010. This finding underscores the inherent complexity of managing and measuring operational risk, and strongly suggests that there is still room for improvement in this area.

Other survey highlights

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

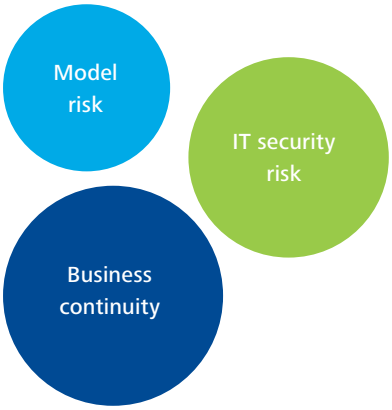
- ***Improvement in risk management capabilities:*** Almost three out of four risk managers rated their institution as either extremely or very effective at risk management overall, an increase from 66% in 2010's survey results.
- ***Firms continue to invest in risk management:*** Two- thirds of financial institutions (65%) reported an increase in spending on risk management and compliance, up from 55% in 2010. The majority of institutions participating in the survey (58%) plan to increase their risk management budgets over the next three years, with 17% anticipating annual increases of 25% 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% of institutions rate their technology systems as extremely or very effective, while 40% 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% of institutions incorporate risk management into performance goals and compensation for senior management, which is little changed from 2010.

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—which ranked near the bottom. In each case, only half of the participants judged their organisations to be effectively managing those risks.

Three emerging risk areas



The strategic importance of risk management and the potential for reputational harm were flagged by the 94% 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

Model risk management

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 breaches 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 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 US$217 million in investor losses that were repaid along with an additional US$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 the inconsistent specification, application and implementation of a model. This applies not only to model-driven trading strategies, but also to quantitative models used for 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% of our survey respondents who said model risk was now included in their ERM programme coverage, only 50% believe they are effectively managing it.

Industry response: our experience

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 utilising stress and back testing.

Deployment and maintenance

Many firms are enhancing the process and rigour 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 the architectural modifications required to support model deployment.

Cyber security and data privacy

Cyber threats continue to evolve in a number of different 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 that hold personal and financial information, as well as intellectual property that can be monetised into huge sums on the black market. Attackers may have significant resources at their disposal (organised syndicates and potentially state-sponsored groups), taking advantage of 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, as evidenced by recent denial of services attacks that caused disruption to financial services institutions' consumer-facing websites.

In the past, it was a common understanding that many threats arose from insiders. However, the figure of 40% for breaches in which attackers gained access through third-party systems should catch investment managers' attention.

This reinforces the need for investment managers to understand their extended enterprise and the control frameworks that service providers have in place to address cyber security

Industry response: our experience

A 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. Analysing the organisation's internet-facing systems
2. Identifying indications of existing system compromises
3. Assessing sensitive data across the organisation and whether it is vulnerable to internet access
4. Analysing vulnerabilities related 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.

Superstorm Sandy and subsequent regulatory scrutiny have prompted many firms to re-evaluate or adjust their strategies for dealing with extended disruptions

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 had been made, which is most likely accurate, but Superstorm Sandy brought BCM practices back into the spotlight for many financial services organisations.

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, whereby only 52% 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:

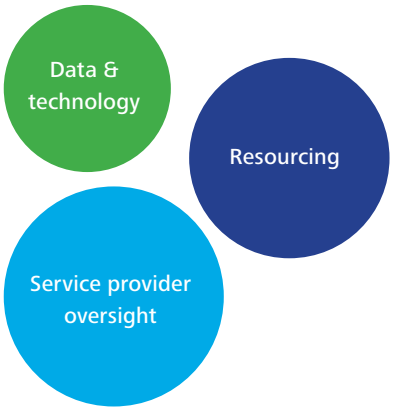
- Scrutiny of vendors, with a rating assigned to them on their BCM preparedness
- Logistics such as communication plans and the need for alternative locations, particularly plans that take into account the possibility of a geographically widespread outage
- Regulatory compliance, particularly in being 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 the aftermath of Superstorm Sandy, we have seen BCM and disaster recovery become a matter for the risk committee, which, in some cases, has even been elevated to board level. Many firms are re-evaluating or adjusting their strategies for dealing with extended disruptions, as Superstorm Sandy provided a number of data points to gauge the effectiveness, in practice, of existing plans, as well as employee response. 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.

Responding to key challenges

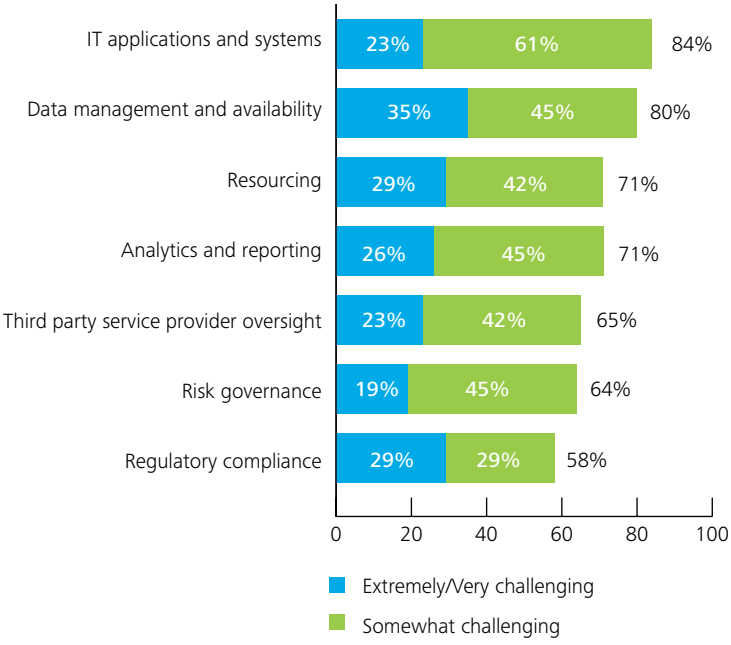
We have discussed some of the emerging risks facing our industry, but our survey also highlights a variety of challenges and inhibitors to managing risk effectively that are specific to firms providing investment management services. These range from data and technology, resourcing and service provider oversight. We have selected a few of these challenges to explore further.

Three key challenges



How challenging are each of the following for the investment risk management function in your organisation?

Risk management challenges



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 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 the reliance on service providers for technology and data. Data quality and consistency can be somewhat problematic as a result, as evidenced by the 79% 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 the ability of organisations to assess, monitor and mitigate risk.

An area of considerable concern across the financial services industry is reference data. For investment managers in particular, the financial downturn exposed both the challenge of 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 proposed a federated approach to distributing LEIs. Subsequent phases of 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 at a significant cost: not only will reference data need to be mapped and transformed, but existing data stores and operational, accounting and risk infrastructure will need enhancement to accommodate the LEI.

There are also increasing technology and data needs associated with investment compliance monitoring in light of the impact on the investment management industry of the recent introduction of the Foreign Account Tax Compliance Act, Form PF and the Alternative Investment Fund Managers Directive. It is therefore unsurprising to see that more than three quarters (78%) of respondents are concerned about the ability of their technology systems to adapt to regulatory requirements. These significant regulatory changes require coordinated cross-functional efforts from the risk, compliance and IT functions, as well as from 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. It can often be extremely difficult to effectively gauge the ROI upfront in respect of the implementation of 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 said, it appears that 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

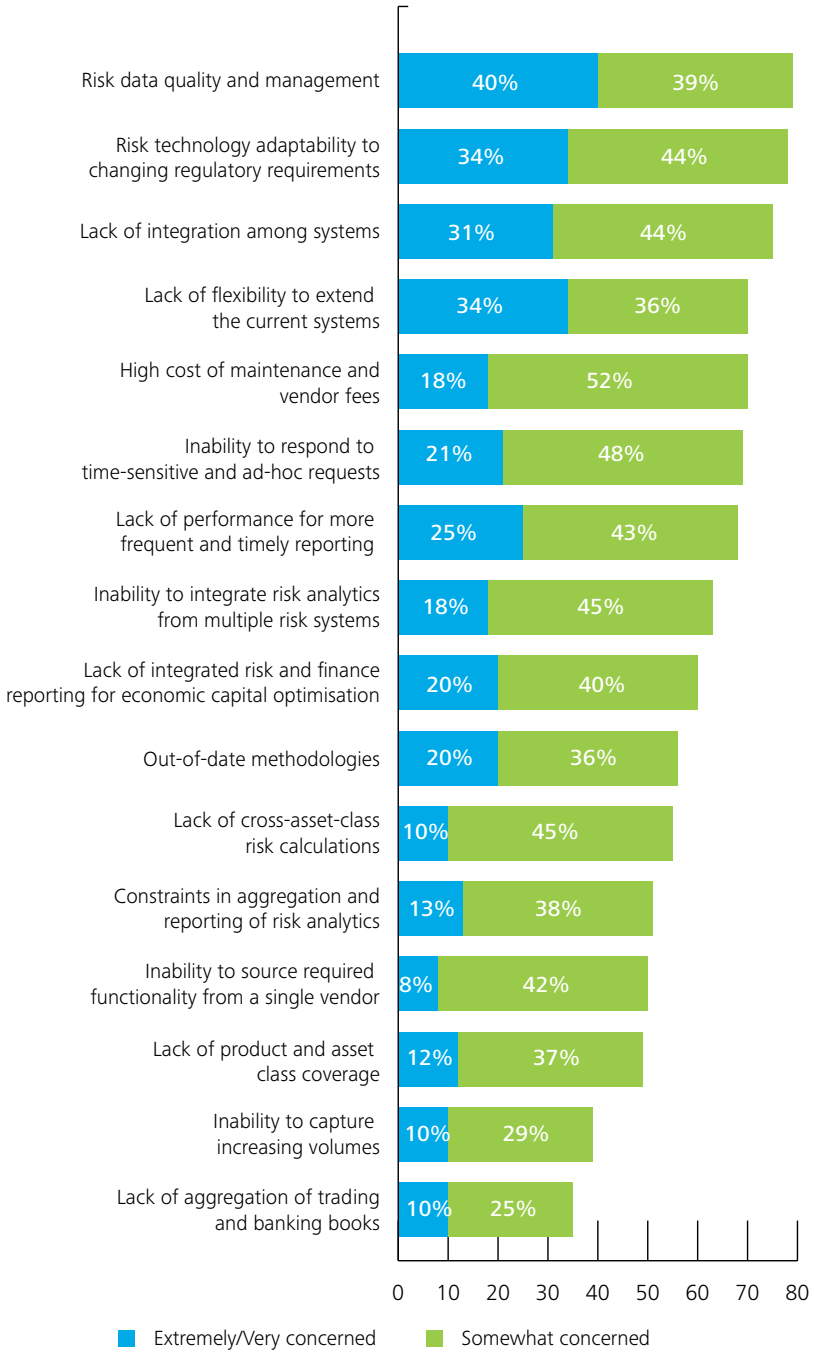
To address deficiencies in infrastructure, a chief goal of the investments that firms are making is to improve the quality and consistency of risk data, with nearly half of those surveyed (46 per cent) planning to make significant investments in this area over the next 12 months. In fact, data-driven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

In our experience, the 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 organisations 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 proved to be a 'silver bullet' to solving risk data quality issues. One of the biggest challenges to improving and maintaining data quality is to make sure it is already 'clean' and accurate when it is placed in the data warehouse.

Even though tools to catch errors on input, such as missing or inaccurate data fields, have been available for some time, many organisations have not implemented error detection processes or assigned responsibility for data quality. As a result, data governance is emerging as an important area of focus for investment managers so that these issues can be addressed. The chief data officer is a position we are seeing 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 visualisation, and the 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, technologies 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 visualisations that can be refreshed intraday, providing proactive support for the decision-making process.

These investments primarily seek to improve and enhance the capability 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.

How concerned is your organisation about each of the following issues for its risk management information technology systems?



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% of respondents consider resourcing to be a somewhat or extremely/very significant challenge.

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 maximise the impact and value to the firm. The growing use of formal risk assessments has empowered organisations to compare and contrast risk exposures across areas that were traditionally managed in silos. As a result, resource allocation decisions that were historically determined by the loudest voice in the room or the potential for revenue generation can now be made with a more holistic view of organisational exposure (where the risk lies) and the ability to realise the strategic goals of the organisation. It has also highlighted skill-set gaps (industry-based and competency), leading to more informed hiring decisions and more effective management of key risk areas. In short, risk-based resourcing is levelling the playing field and delivering enhanced allocation of a firm's most precious resource—people.

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 (e.g. of 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 non-performance and have strengthened their vendor risk management programmes accordingly. Thus, 40% of firms believe they have high potential exposure to the risk of non-performance by their custodian and 35% attribute this risk to their administrator. In addition, 23% and 20% felt they had high exposure to potential non-performance by their prime broker and transfer agent respectively, while only 13% felt they had high exposure to potential non-performance by their distributor.

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 gain a better understanding of the risk profile of each service provider. In addition, they are establishing a service provider oversight framework aligned with their overall risk profile, which 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 created 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 programmes to incorporate a diverse pool of providers that do not necessarily conform to standard contracting practices and supplier/buyer influence and leverage norms.

A forward-looking assessment of risk

Investment managers, like many of their counterparts in the broader financial services industry, are working to enhance and identify their management of 'traditional' risks, as well as those that are growing in importance or rapidly emerging. When discussing risk with our investment management clients the key question seems to be: what is the most efficient and effective way to target our risk management efforts?

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 face—so they can concentrate more on growing the business and generating superior returns.

To the **point**:

- In whatever manner a firm is addressing its risk, our survey results indicate that investment managers are elevating the discipline of risk management and are turning to technology and advanced data solutions to increase their effectiveness
- There is still work to be done to both head off emerging risks and address challenges that are inhibiting traditional risk management approaches
- More experienced risk managers are taking the time to examine the nuances of their firm's risk culture by devising new and improved ways to measure risk-taking throughout their organisations and stressing the need for greater organisational awareness and integration across risk, IT, operations, compliance, internal audit and legal functions

When discussing risk with our investment management clients the key question seems to be: what is the most efficient and effective way to target our risk management efforts?