Inside

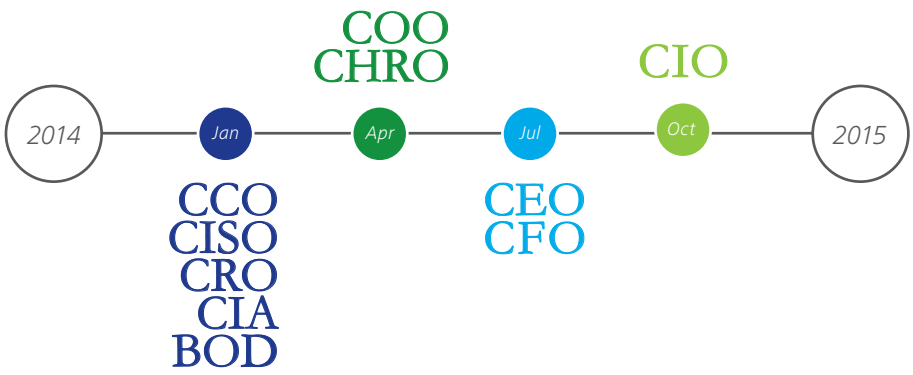
CCO
CISO
CRO
CIA
BOD

EDITION
2014

Deloitte.

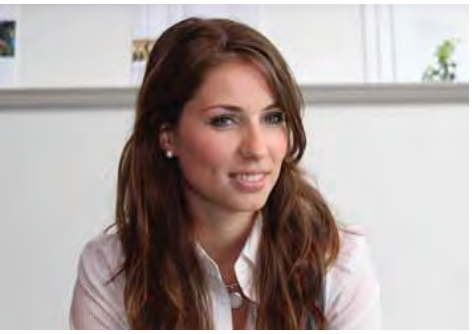
In this issue

Each edition of the magazine will be addressing subjects related to a specific function.
Please find below an overview of the spotlight for the upcoming editions of the magazine:



46 52 56 62 68 78 82 86 90

Foreword



Firstly, we wish you and your family all the best for the New Year.

This is the third edition of our In*side* Magazine, a quarterly publication launched in 2013 aiming at sharing insights across business functions and various industries with you. In*side* Magazine will provide you with our main points of view and give you access to whitepapers and studies across all industries, with a particular focus on:

- Business & Regulatory Strategy and Corporate Finance
- Operations and Human Resources
- Information Technology
- Internal Audit, Compliance, Risk Management, Board and Board Committee member's issues

This edition of the magazine focuses on the roles and challenges of Chief Risk Officers, Chief Information Security Officers, Chief Compliance Officers, Chief Internal Auditors and Board Committee members. In*side* aims at becoming a platform for sharing knowledge, experiences and expert advice on topics and issues encountered, regardless of location or industry type. We hope that you enjoy this new edition, which provides an international flavour thanks to contributions from experts in our worldwide network.

Our goal is to enhance the creativity and innovation of this publication. We therefore welcome any comments or suggestions for future topics or article contributions and would be glad to receive your views and ideas on any subject treated in the magazine.

We hope you enjoy this edition and look forward to hearing from you soon.

Joël Vanoverschelde
Partner
Advisory & Consulting
Deloitte

Pascal Martino
Director
Advisory & Consulting
Deloitte

Julie Chaidron
Manager
Advisory & Consulting
Deloitte

Editorial

With today's heightened awareness of the need for anticipating and managing risks in an ever-more dynamic and uncertain environment, boards, audit, risk and compliance committees and C-suite executives are striving to better understand the broadest range of their actual or potential risk exposures and the effectiveness of their governance, risk, and compliance infrastructure.

For this reason, we have chosen to dedicate this third edition of In*side* magazine to the wide range of professionals involved in governance, risk management, compliance and internal audit issues.

Indeed, governance and risk management remain some of the most compelling issues of our time and are firmly at the top of the agenda. This is not only the result of it being one of the most prominent features of the regulatory landscape in many industries, but is also simply because the crisis has shown that conventional risk management and risk oversight have failed in the modern world where risks (e.g. disruptive technological shifts, cyber-crime, economic trends and evolving business models, regulatory sanctions, instantaneous global communications through social media, etc.) strike with a much greater impact and at a much higher speed of onset than in the past.

As we all know, there is no way to completely shield an organisation from the world's uncertainty and turmoil. However, there is what we at Deloitte call a 'Risk-Intelligent' path. There are also ways to enhance value and manage risks that enable better decision-making and therefore maximise the likelihood of resilience and sustainable success.

In this edition we have gathered a series of articles written by a selection of some of our most prominent worldwide Enterprise Risk Services specialists. These authors have pooled their expertise to help Boards of Directors, Board Committees, Chief Risk Officers, Chief Information Security Officers, Chief Compliance Officers and Chief Internal Auditors bring more clarity and effectiveness to their risk governance and risk management activities.

We hope you will find this publication insightful.

Thank you for your interest and support.

Laurent Berliner
Partner
EMEA Financial Services Industry –
Enterprise Risk Services Leader
Deloitte

Jean-Philippe Peters
Director
Business Risk
Deloitte

Please contact:

Laurent Berliner
Partner
EMEA Financial Services Industry
Enterprise Risk Services Leader
Tel: +352 451 452 328
Mobile :+352 621 184 667
lberliner@deloitte.lu

Jean-Philippe Peters
Director
Business Risk
Tel: +352 451 452 276
Mobile: +352 621 251 230
jppeters@deloitte.lu

560, rue de Neudorf, L-2220 Luxembourg
Grand Duchy of Luxembourg
www.deloitte.lu

The changing world of strategic risk

Henry Ristuccia
Global Leader
Governance, Risk and Compliance
Deloitte

Aida Demneri
Director
Risk Services
Deloitte

Effective risk management has always been the cornerstone of the most successful companies. But in today's risk-filled business environment, it can be difficult for executives to assess whether their plans and strategies can be executed as anticipated. One of the main reasons is that strategic risks—those risks that either affect or devolve from business strategy decisions—can strike more quickly than ever before. The catalyst behind that reality is frequently new, rapid-fire business trends, as well as technological innovations such as social media, mobile and big data. Companies that fall behind on the innovation curve may quickly fall prey to innovation's evil twin-disruption. That is just one of the several reasons why managing strategic risk has become such a high priority for many executives, worldwide. The fact is that today risks strike at a much greater speed. That is why companies have to be better prepared and ready to respond much faster than they might have been even just three or four years ago.

In a recent study, we uncovered significant and compelling evidence that many businesses around the world are adopting a new view of the risk universe. The study, conducted in spring 2013 by Forbes Insights, on behalf of Deloitte, was a global survey of strategic risk management practices at more than 300 major companies worldwide. In the survey, Deloitte had one major objective: to better understand how businesses can manage strategic risk more effectively—both now and in the future. The survey set out a wide range of issues and questions, such as:

1. **To what extent are companies considering and addressing risks as they develop and evaluate their business strategies?**
2. **What new risks do their strategies create?**
3. **Which strategic risks are critical to avoid or essential to take?**
4. **What is the strategic impact of new technologies, and which investments are essential to managing risks and exploiting new opportunities?**
5. **And, even if a company's strategy is executed flawlessly, what other risks could undermine the business?**

More broadly, the main areas of the survey covered the alignment of strategy and risk, the monitoring of strategic investments, and the emerging views of strategic risk management.

While some findings reinforced what many already believe, there were also some surprises. Here are a few of our key findings:

Most companies are doing more than just making strategic risk management a higher priority

Importance of strategic risk

Strategic risk has become a matter of substantial focus for companies. 81% of the companies surveyed are now explicitly managing strategic risk. In addition, many companies are adopting a broad view of strategic risk that goes beyond a focus on challenges that might cause a particular strategy to fail. They are also weighing any major risks that could affect a company's long-term positioning and performance.

A higher priority

Most companies are doing more than just making strategic risk management a higher priority. They are also changing the very way they manage strategic risk. In fact, nearly all respondents (94%) have changed their approach to strategic risk management over the past three years. The numbers were slightly higher in Asia/Pacific (96%), and slightly lower in Europe/Middle East/Africa (EMEA) (91%).

Progress made

A key improvement noted by the survey is that more and more companies are integrating strategic risk analysis into their overall business strategy and planning processes. And that integration appears to be working. Among the companies surveyed, 61% now believe their risk management programmes are performing at least adequately in support of the development and execution of their business strategy. But that's only part of the story. According to the overall results, only 13% of companies rate their risk management programmes at 5 out of 5 in terms of supporting the development and execution of strategy.

A matter for the CEO and board

Strategic risk management is a CEO and board-level priority. Two thirds (67%) of the companies surveyed say that the CEO, board, or board risk committee has oversight of strategic risk management. In EMEA, CEO direction is much lower than average and board direction is higher. Top-level oversight is particularly common at consumer companies, followed by companies in financial services and technology, media and telecommunications.

An executive of one large European conglomerate explained how risk management policy is set by the managing board. "*Our risk management policy is set by our managing board*", says Siemens AG's Dr. Georg Klein, Chief Risk & Internal Control Officer, Corporate Finance and Controlling. "*On the other side, the organisational and accountability structure is primarily based around Siemens' four sectors: energy, industry, infrastructure & cities and healthcare. Sector managers, together with regional clusters and corporate units, implement risk management programmes that are tailored to their specific industries and responsibilities, yet consistent with the overall policy established by the managing board*."

Reputation

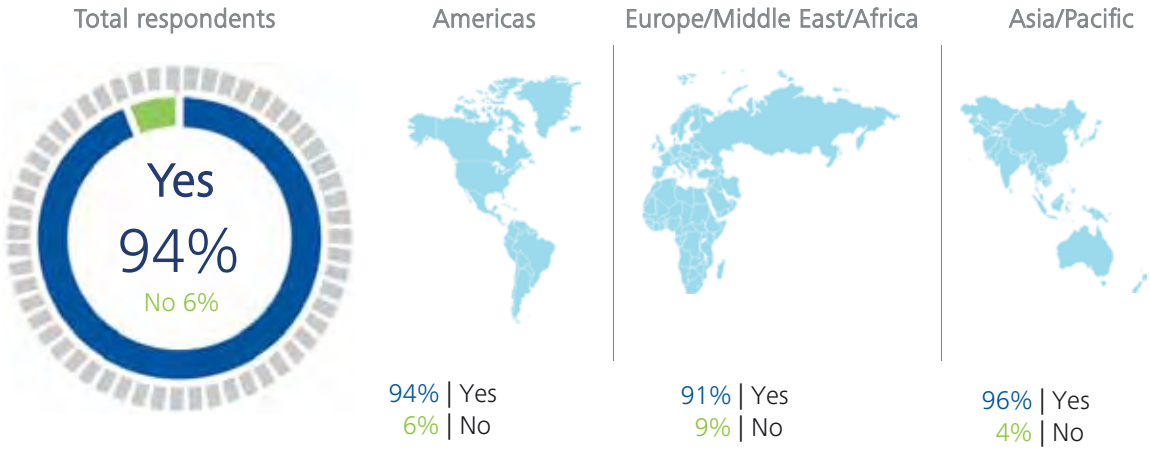
Reputation risk is now the biggest risk concern. That fact is due in large measure to the rise of social media that enable instantaneous global communications. These media make it harder for companies to control how they are perceived in the marketplace. The emergence of new communication vehicles, such as mobile and social networks, has given rise to concerns that new forms of communication may impact corporate reputation in different and faster ways than ever before. Hence the need to monitor these vehicles and the content they carry to accurately anticipate and proactively control the emerging risk.

According to the companies interviewed, social technologies are one of the main factors driving rising concerns about reputation. Given the speed and global reach of social media, companies today are at much greater risk of losing control over how they are perceived in the marketplace. As a result of the rise of social media, reputations built up over decades can be challenged or undermined in an instant. Customers frequently make decisions about an organisation based on social media comment, and sometimes well before any corporate team can intervene to defend the organisation or formulate a response.

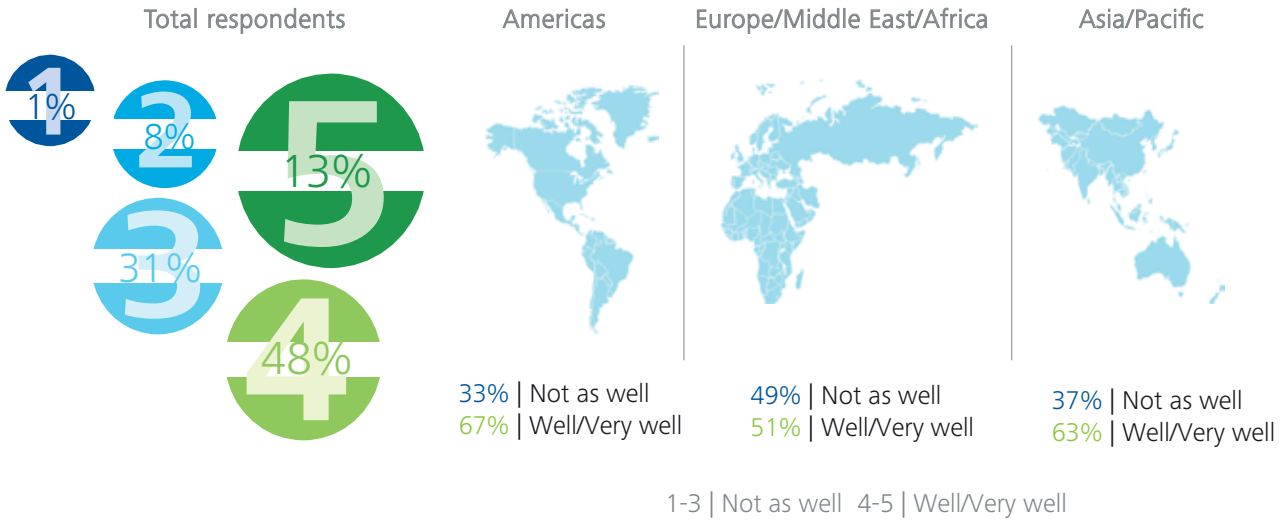
Impact of technologies

Technologies are also having a major impact on the business and risk landscape. The majority of the companies surveyed (53%) believe technology enablers and disrupters such as social, mobile and big data could threaten their established business models, and 91% have changed their business strategies since those technologies began to emerge. New technologies have had their biggest impact in three sectors: technology media and telecommunications (97%), consumer and industrial products (96%) and life sciences (94%). Regionally, the largest impact was in Asia/Pacific, where 98% of respondents report having changed their business strategies.

Q: Has your approach to managing strategic risks changed in the last three years?



Q: On a scale of 1 to 5, how well do you think your risk management programme supports your ability to develop and execute your business strategy? (5 indicates very well)



Q: Which of the following risk areas have the most impact on your business strategy (three years ago, today and three years from now)? (Respondents could choose more than one answer. The top three are shown below)

2010	Today	2016
41% | Brand	40% | Reputation	29% | Economic trends
28% | Economic trends	32% | Business model	26% | Business model
26% | Reputation	27% | Economic tends | Competition	24% | Reputation | Competition

Human capital and innovation

Three years from now, human capital and the innovation pipeline are anticipated to be the top strategic assets in which businesses will need to invest. Many respondents (47%) view human capital—that includes employees, partners, and contractors—as a strategic asset worthy of investment. The innovation pipeline is another strategic asset closely related to human capital. Again many respondents (23%) consider it a worthy investment. In addition, many respondents (26%) view customer capital as an important area of investment. Three years into the future, we anticipate that the innovation pipeline will emerge as a top risk-related strategic asset in which to invest.

Clearly, in an era in which risk can become reality in the blink of an eye, companies need new capabilities and approaches for managing strategic risk. In particular, they should now weigh and assess a much broader set of risks and strategic assets. That set should include, but should not be limited to, people, intellectual property, customers, marketing efforts and even 'the crowd'. These risks and assets are much more difficult to measure, capitalise on and hedge against. For that reason, they demand a much more systematic and sustained approach to monitoring and managing risk.

In order to address the risk challenges of tomorrow today, companies must also reach outside of their traditional corporate structures to adopt a more 'outside-in' perspective when assessing their strengths, challenges and opportunities. This will require a new commitment to gathering data and appreciating external perspectives from 'outside' sources. That includes customers, bloggers, information trend setters, and marketplace and security analysts. It will also require learning from other companies and industries.

We have witnessed an information explosion in the past decade—what Tom Friedman of 'The New York Times' has called "*the Great Inflection*"—a hyper-connected world grounded in social media, cloud computing, 4G wireless, ultra-high-speed bandwidth, System-On-a-Chip (SOC) circuits, mobile devices, tablets, etc. Managing risk in this new business universe requires much more than listening to customer feedback. The accepted information hierarchy, including established newspapers and media outlets, has rapidly given way to a multidimensional information matrix where no single voice dominates. Information and opinions of all kinds are easier to access, yet more difficult to evaluate and control. In response to these new realities, companies are making a deliberate effort to improve their strategic risk management capabilities and performance.

Traditional approaches to managing risk tend to concentrate on monitoring leading financial indicators in addition to the evolving regulatory environment. Yet, given that they are generally grounded in audited financial statements, the risk strategies and hedges that result are in large measure a reaction to past performance or negative events. They do not, however, necessarily serve to detect future strategic risks or predict future performance. For that reason, they are more focused on protecting value than on creating it. Given the result of this survey, we are confident, however, that the traditional approach is quickly giving way to new and innovative approaches to strategic risk management—approaches that are much more focused on the future.

This piece draws heavily on "Exploring Strategic Risk 300 executives around the world say their view of strategic risk is changing", Deloitte, 2013. For information, contact Deloitte Touche Tohmatsu Limited or visit www.deloitte.com/strategicrisksurvey.
Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing, p. 8

Aligning risk and the pursuit of shareholder value

Risk transformation in financial institutions

Scott Baret
Global Financial Services Leader
Enterprise Risk Services
Deloitte

Financial institutions of every type face continuing pressure from regulators on one side and shareholders on the other. Working to balance the former's expectations for higher levels of capital and the latter's for superior returns, senior executives and boards are deploying ad hoc, piecemeal responses to financial regulation that—in the long run—only increase costs and perpetuate risk.

These challenges impact senior executives and boards at banks, insurers, broker dealers and other financial institutions across multiple lines of business. While global systemically important financial institutions (G-SIFIs) and SIFIs may be most affected, virtually all national and regional institutions also face similar challenges, if on a different scale. Most financial institutions, however, are overlooking opportunities to holistically address capital efficiency demands by integrating financial, risk and regulatory data streams.

To bring light to these opportunities and begin answering some of the most common issues faced by financial institutions, Deloitte recently published "*Aligning Risk and the Pursuit of Shareholder Value*". The paper presents an analysis of forces impacting shareholder value and the 'transformational moves' that executives and boards should consider when aligning their risk management strategies and operations.

To aid financial institutions in identifying the need for transformation, the paper provides a business case for aligning risk to the pursuit of shareholder value, as well as an overview of the four cornerstones of risk transformation.

The business case for risk transformation: four key drivers

1. Scarce capital, liquidity and funding

Financial institutions must remain competitive while maintaining increasingly high levels of capital as regulatory agencies introduce increasingly stringent supervisory requirements. These needs are compelling the industry to rethink and reconfigure business models, governance processes and risk management capabilities.

2. Extensive industry and regulatory requirements

Global financial institutions with multiple lines of business must respond to a myriad of jurisdictional regulatory requirements. Too often these requirements involve redundancy, overlap, and increased compliance costs and risks. Addressing these requirements calls for global coordination of regulatory compliance and risk management resources.

3. Rising costs and performance pressures

With significantly higher capital requirements due to Basel III and other regulations, the cost of existing business models may continue to rise, eating into margins. To sustain strong earnings, institutions have begun to de-emphasise certain businesses, while emphasising others, reducing costs, and in some cases pursuing new strategies. Such responses can, however, introduce new and potentially dangerous concentrations and combinations of risk, as well as add new costs.

4.Legacy infrastructures

Legacy systems and hardware platforms are likely to present high barriers to effective compliance, risk management and business management. A well-conceived enterprise risk data architecture can help overcome these barriers by making it possible to build the right data repositories and to avoid bolted-on regulatory solutions. An integrated enterprise solution specific to the institution can improve data quality, accessibility and analysis, setting the scene for improved risk management and business management.

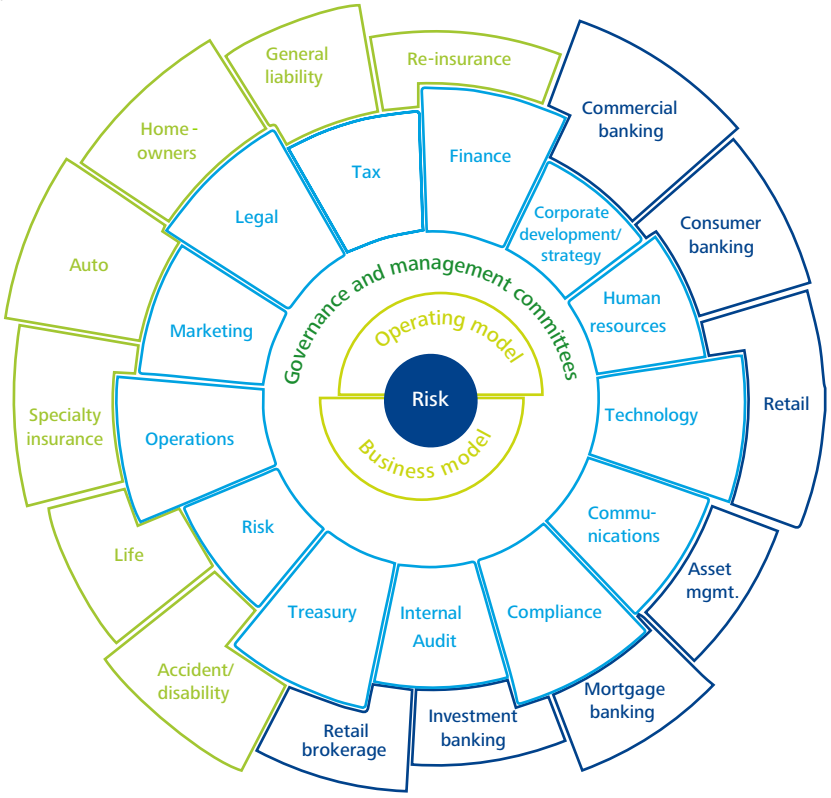
Impact on drivers of shareholder value

Shareholder value is driven principally by achieving a positive spread between the risk-adjusted return on capital and the cost of capital, and factors such as operating costs and taxes. These drivers are impacted by specific forces and market conditions affecting the business. A focus on shareholder value highlights the need to meet regulatory expectations while simultaneously improving operations management and risk management. This approach transforms the need to meet regulatory expectations in areas such as capital planning and management, stress testing, business conduct, organisational culture, risk data management and risk management into opportunities to improve these capabilities from an operational standpoint and further integrate risk management practices into business unit processes and activities. Similarly, regulatory demands pertaining to risk-based capital requirements could present opportunities for management to relate risk to capital more strategically. Doing so is likely to enable management not only to justify capital allocation and obtain business unit buy-in, but also to deploy capital more effectively for higher investor returns.

Needs vary by organisation, and specific responses will be particular to the institution. In general, however, certain approaches will be more likely than others to generate effective responses to regulatory expectations and deliver improvements in business results. These approaches embed risk management into business units and functions at the level of people's daily responsibilities. When that occurs, risk management is no longer considered just the responsibility of the risk management function but an integral part of the job of the trader, loan officer, underwriter, portfolio manager, claims manager, HR professional, IT specialist or other personnel.

This said, maintaining historical returns under today's uncertain conditions is challenging. Thus, management should take a holistic approach to these challenges, which may represent a break with the past. In most institutions, siloed responses to regulatory changes, economic indicators, shareholder demands and risk have generated a lack of alignment, with results that can resemble aspects of the structure depicted in Figure 1. In such organisations, although they are centred on risk, business models and operating models are not aligned, nor are the business units and functional areas. Risk management lacks coordination, and business units and functions may see risk as the responsibility of the risk management function rather than intrinsic to their jobs.

Figure 1: Lack of alignment in a financial institution

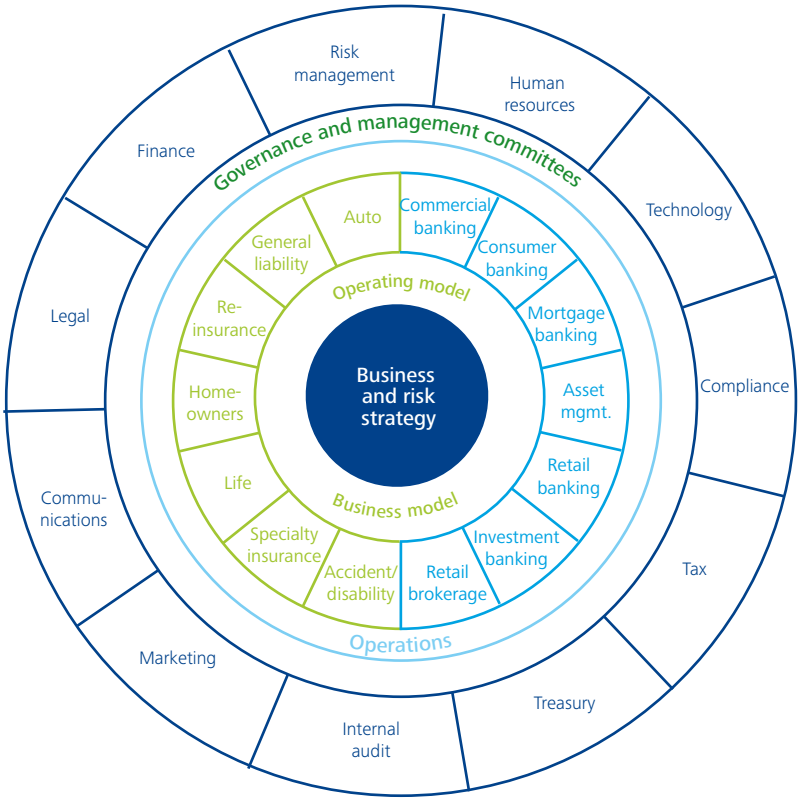


Misalignment and gaps develop over time, sometimes over decades, as an organisation diversifies its businesses, introduces new products and services, and responds to new laws and regulations. Some business units come to see the risk management function as being responsible for managing risk, whereas the risks actually reside in the businesses. The resulting lack of alignment may leave institutions unintentionally exposed to risk and unable to efficiently coordinate responses to regulatory change. Lack of alignment also results in fragmented technology systems and data repositories, inhibiting the organisation's ability to manage enterprise risk cost effectively and respond to regulatory demands.

An aligned organisation (as illustrated in Figure 2) should integrate business and risk strategies and explicitly task risk owners with both organisational objectives and risk management responsibility. Risk owners should manage the full range of risks they face and be supported by a suitable risk management infrastructure. The businesses and functions—and executives and the board—should fulfil their risk-related responsibilities in ways that align regulatory and other stakeholder expectations. This aligned organisation should minimise silos and fragmentation among business and risk strategies, business and operational models, and businesses and functions. It should be supported by a common operational and risk data architecture. This should enable the institution to access specific data when needed and to drive down costs by embedding risk management and regulatory IT support into the broader strategic technology architecture.

An aligned organisation should integrate business and risk strategies and explicitly task risk owners with both organisational objectives and risk management responsibility

Figure 2: Alignment in a financial institution



This illustration of alignment is **not** presented as a model or framework, but is simply meant to portray the integrated state of an organisation aligned around business and risk strategy. The result is greater synchronisation between strategy and execution in operations and risk management.

How is such an integrated state achieved?

Risk transformation: a path to alignment

The desired state is most likely to be achieved through a process of risk transformation. Risk transformation integrates risk management into the conduct of business, taking risk management to higher levels of excellence by driving practices throughout the organisation. This means embedding risk management in the daily activities of employees so as to align the conduct of business and of risk management with the businesses strategies.

Risk transformation takes the need to respond to regulatory change as an opportunity to strengthen not only the management and governance of risk, but also the management of capital and operations and the supporting IT infrastructure. For instance, regulations impact business models, pushing management to choose which businesses to pursue, what scale to achieve, and how to manage risks and capital in the businesses. Those choices are best made from a holistic point of view with due consideration given to the enabling data and analytical resources.

In an aligned organisation, risk management and governance acknowledge business unit and overall ROI objectives and the risk profile required to achieve those objectives. This aligns operational and risk management and risk governance policies, practices, roles and responsibilities. The risk management function then supports each business in operating within the risk profile each requires in order to meet return objectives.

In the desired state, risk is identified at its source and managed within business activities. To the appropriate extent, accountability for risk management shifts to the businesses and functions, while responsibility for risk is shared among the businesses, functions and risk management. This enhances the visibility on risk of the businesses and functions and the visibility of aggregate risk positions, with the potential to improve decision making in the businesses and functions and at the organisational level.

Four cornerstones of risk transformation

To translate the overall goal of achieving alignment as described here into actionable focus areas, four organisational components—or cornerstones—of risk transformation have been identified. These cornerstones highlight cross-functional, risk-related elements and activities that help determine an institution's approach to risk.

If management firmly establishes these cornerstones, risk management and regulatory compliance efforts have the potential to be implemented in an efficient, coordinated manner within each business and across the organisation.

The four cornerstones of risk transformation	
Strategy	Strategy puts the organisational vision and mission into action. The executive team should consider the risks of the strategy and to the strategy, as well as the regulatory implications of a strategy. Transaction and portfolio risks and individual and aggregate risk exposures should be well understood. Enterprise risk management and governance infrastructures should support execution of the business model and capital allocation. Capital is allocated based on strategically selected risk-reward trade-offs, risk capacity and appetite, and the desired risk profile.
Governance and culture	Governance is intended to ensure that strategies are executed properly and in alignment with risk and business strategy. Culture embodies the shared values, principles and beliefs that guide the organisation. Governance and culture set expectations regarding risk taking and risk management, enabling people to discern acceptable and unacceptable risks even when they are not explicitly covered by policies and procedures. In considering governance and culture, the executive team might assess the organisation's level of risk intelligence, its risk management and governance frameworks, and its risk governance operating model.
Business and operating model	The business model defines economic relationships between the organisation and its customers, suppliers, investors and other stakeholders. The operating model structures the ways in which the business conducts its activities with its stakeholders. Within both models, risk should be managed with clear accountability, authority and decision rules at all levels, and well-defined handoffs between business risk and control functions. Both models require standardised structures, processes and controls for shared and outsourced services, as well as for business units and support functions.
Data, analytics, and technology	Management should determine the key data required to address risk management needs and oversee development of a data management and sourcing strategy to address those needs. Management should also facilitate integration of finance and risk data to enable common and reconciled risk and regulatory reporting. The business units need near real-time processing and reporting of aggregated risk data to monitor volatile liquidity, market and credit risks. An enterprise risk data and architecture strategy can deliver the right risk-related data to the right points and enable the institution to respond to new business opportunities and to risk and regulatory demands consistently and efficiently rather than through ad hoc or bolted-on solutions. A streamlined set of business intelligence solutions can support risk and regulatory needs, while analytics enable scenario analyses of stresses on global positions.

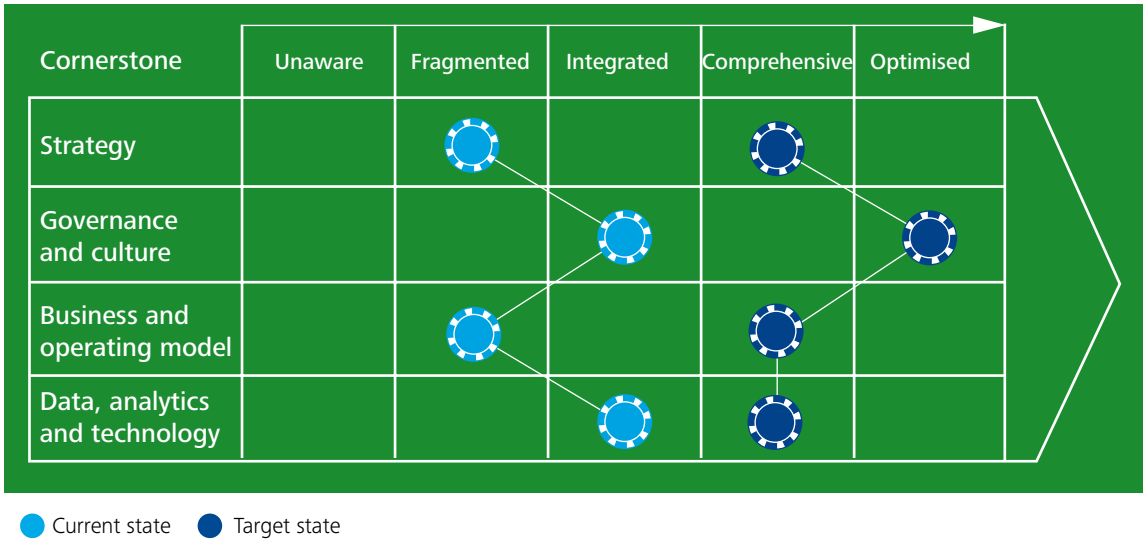
The risk management function then supports each business in operating within the risk profile each requires in order to meet return objectives

Assessing needs

As noted, the risk transformation journey differs for each organisation. In defining the future state of the organisation, executives might assess the current state in terms of these cornerstones (see Figure 3). They can then decide which capabilities related to strategy, governance and culture, business and operating models, and data, analytics and technology require what degree of enhancement. As shown in the chart below, risk transformation helps leaders define subjects for analysis across the organisation against a maturity continuum. Five distinct maturity states are defined for each cornerstone, with the 'optimised state' corresponding to the practices of a 'risk intelligent enterprise'.

Risk transformation recognises that risk management can be organisationally aligned even if parts of the whole stand at various maturity levels. The maturity continuum is only one tool by which risk transformation assists management in identifying, categorising and prioritising activities for enhancement. Primarily, the cornerstones—and the concept of risk transformation—aim to elevate senior-level discussions regarding risk management, risk governance and regulatory compliance.

Figure 3: Example of a maturity continuum



Five distinct maturity states are defined for each cornerstone, with the 'optimised state' corresponding to the practices of a 'risk intelligent enterprise'

Given the nature of the changes, here are some key points to consider, framed as questions to be answered in senior-level discussions of risk management and regulatory compliance:

- **Strategy**
  How clear are our business and risk strategies to internal and external stakeholders? How can we improve that clarity? How can we bring our risk strategy more in line with our business strategy so they support one another? How can we allocate capital more efficiently while managing the risks to which it is exposed? How much capital should we allocate to new business initiatives?
- **Governance and culture**
  Do our governance systems and culture support implementation of our strategy? How can we best align our governance goals and our organisational culture with our values and mission? To the extent that we see misalignment, what is the cause? What values are, and are not, expressed in our culture? How can we drive positive values throughout our culture? Are we truly practising good governance?
- **Business and operating models**
  How can we best drive awareness of and accountability for risk throughout the organisation? To what extent have we rationalised, synchronised and optimised risk management and regulatory compliance mechanisms? How could we enhance these attributes? How can we achieve regulatory compliance without disruption to our operations? Is it possible for a unit to engage in risky activity without the knowledge of the board and the management?
- **Data, analytics and technology**
  How can we leverage our investments in risk management, internal control, and data management and analysis? How can we better align these across our organisation? How well do our data management and analytical capabilities support our risk management and regulatory reporting efforts? How can we develop an integrated data storage and aggregation infrastructure to support financial, operational, regulatory and risk reporting?

There are many other questions, but the above selection makes a good start. And the time to start is now.

Corporate governance trends and challenges for board members

Dan Konigsburg
Managing Director
Corporate Governance & Public Policy
Deloitte

Corporate governance has grown up. Over the last decade, the debate about governance has evolved from a specialised concern of activist investors and business school professors into a legitimate concern of boards and board effectiveness.

The financial crisis has, in many countries, pushed governance questions onto the front pages of newspapers and regulators have asked more difficult questions about how boards of directors provide oversight over business models, risk-taking, strategy and long-term business sustainability. Along with the increased visibility of corporate governance, we have witnessed a similar expansion in the range of issues taken up by boards. We are no longer talking about whether or not boards should include an audit committee or independent directors: in the current climate we are grappling with the issue of what makes a board effective, which raises a much more meaningful set of questions.

What makes an effective board?

There may be as many answers to this question as there are different types of companies. Yet we can see the broad contours of common themes emerging as countries around the world as distinct as France, Japan, Singapore and the United States engage in similar discussions.

One of these themes is **independent directors**. Yes, we are long past the point in most countries where the value of independent directors needs to be proved (although, as is so often the case, Japan remains an exception; the very idea of independent directors remains a controversial one and many listed companies include no outsiders on their boards). Meanwhile, the number of independent

directors on boards continues to increase. In Western Europe, most countries' codes of corporate governance require one-third of directors to be independent. In the UK, it is a clear majority and up to two-thirds of the board; in the U.S., the entire board—apart from the CEO—must comprise of independent directors. Why such a focus on independence? One reason is certainly to ensure management accountability, particularly where there are majority owners. But another reason is to bring an outside perspective into boardroom discussions. Boards without outside directors tend to be confined to operational matters, or simply approve decisions that management has already made; they do not generally contribute to the company's strategy or strategic thinking. Yet independence can have its limits. Some directors have proved so independent that they have little knowledge of the business. The board of Lehman Brothers, for example, had precious few directors with banking expertise—a skill that one assumes might have been useful in early 2008. Some governance observers have begun to argue that the fetish for independent directors has blocked real industry expertise from joining boards, and that what is needed now is a relaxation of independence standards to bring more insight into certain boardrooms.

Director diversity is another factor in board effectiveness. In perhaps the most remarkable governance trend over the last decade, some eight countries have introduced legislation requiring a minimum percentage of women on all listed company boards. Norway's quota was the first to be introduced, in 2006, with 40% of board members required to be women. It was followed by similar quotas in France, Spain, Italy, Belgium and the Netherlands, and in the last year, the European Union as a whole proposed a quota at levels of between 10 and 30%. And the trend is not confined to Europe. In Malaysia, the government has introduced a target of 30% women on listed company boards and India now requires one woman on large, listed boards as a result of revisions made in late 2013 to its Companies Act. However, two questions remain. Why quotas and why now? Some have argued that quotas address the issue of self-perpetuating boards, and force different opinions and perspectives onto a previously homogenous membership. And the issue has appeared recently, one suspects, for several reasons: in part because boards, as currently composed, are seen to have not responded well to the financial crisis. But some momentum is surely driven by the internationalisation of shareholder rolls, and the power of social media and other networks to spark change. The recent trend toward shareholder votes to approve remuneration policy (the 'say-on-pay' vote) has made a similar escape from obscurity in nearly ten countries, it would seem, simultaneously.

Strong **oversight of risk-taking** is surely another component of board effectiveness. In the wake of the financial crisis, investors have asked what responsibility boards have for oversight of risk. Investors and regulators alike have suggested new structures for boards, like a formal risk committee. Here, there are currently more questions than answers: can the audit committee be responsible for both risk oversight and its existing responsibilities? Should the board as a whole be responsible for certain enterprise-wide risks like reputational risk, technology risk or regulatory risk?

How involved in risk is too involved for outside directors? What key risks should management report to the board and how should directors follow these risks and seek accountability from management? Should the board set risk appetite, and how? In the U.S., the Dodd-Frank Act has answered these questions with the requirement that some financial institutions adopt risk committees. The U.S. Securities and Exchange Commission (SEC) now requires disclosure of how the board oversees risk. In Europe, the European Commission completed a consultation in 2012 on this very issue. Singapore is updating its own governance best practice code to clarify that the board is responsible for oversight of risk. Different boards seem to be reaching their own conclusions on these questions and there remains a great diversity of practice. Still, while the answers may differ, we are unlikely to go back to the days where the board could delegate its responsibility for risk oversight to management. At least it is clear today that directors must understand management's system for risk management, and hold them to account for implementing it.

Perhaps the most telling component of board effectiveness is how it provides **oversight of strategy**. As with board involvement in risk management, there are an equal number of questions for boards about how they should be involved, and how deep they should dive. In many countries—and in particular the United States—boardroom culture is such that the board may see its role as the mere endorser of strategy. U.S. boards are not often encouraged to work with management on formulating strategy. In other countries, boards may feel their role is to be deeply involved, together with management, in setting the strategic direction. Many directors wish to constructively challenge management's strategies or their underlying assumptions, particularly where there are links between strategy and risks. The most effective boards will often have a conversation with the CEO and management about what their role in the area of strategy should be. If the board avoids this conversation, management may feel the board is micro-managing, or they may feel the reverse—that the board is abdicating its responsibility. Apart from the level of involvement, the issue of boards and strategy is complicated by the fact that strategy is so often personified by the CEO. Where this is the case, questioning the CEO's strategy can be tantamount to challenging the CEO himself. Some CEOs **are** the strategy. In many cases, the way to avoid misunderstandings is through the use of an emotionally intelligent chairman.

Another marker of an effective board is if it has frequent discussions about **succession and succession planning**. Put another way, weak boards are those which are afraid to bring the subject up in front of the CEO. Shortcomings in succession planning can be among the most distracting, damaging and, not least, the most public of corporate governance failures.

But the broader question of developing management talent is a tricky one for boards. CEO tenures are growing shorter in many countries—and that leaves less time for those lower down the organisation to learn what they need to know before they take over. Strong boards take a proactive approach and get involved. They think about succession in terms of a risk to the organisation. Deloitte suggests four kinds of succession planning risk:

Some chairmen in the United Kingdom and, to a lesser degree, in the United States, see their role as speaking with long-term shareholders as a bridge to management

1. **Vacancy risk:** the risk that a particular position becomes vacant, for whatever reason. The more important the position, the greater the risk
2. **Readiness risk:** the risk that there are no internal candidates to take over a position. If no one is ready to step in, companies may have not one, but two problems: the vacant position and no one to fill it
3. **Transaction risk:** this is the potential for disruption when an executive moves from his current position to the new position
4. **Portfolio risk:** the possibility that the person taking over and stepping into the vacant position does not have the right set of skills to take over effectively

In each of these cases, strong boards of directors engage with the human resources team, often asking for HR presentations at board meetings and reviewing the succession planning process on a regular basis. Effective boards role-play scenarios where they learn how prepared they would be if they lost their CEO unexpectedly. These days, it is no longer sufficient to accept a CEO's assurances that he has 'someone in mind'.

Finally, some boards are beginning to **engage with their investors** more than before. If we have learned anything from the financial crisis, it is that investors can be fickle and may abandon companies in times of trouble. For some companies, the lesson learned has been that you should seek out the shareholders you want. Some chairmen in the United Kingdom and, to a lesser degree, in the United States, see their role as speaking with long-term shareholders as a bridge to management.

But investors can betray a short-term mindset. Some quarters of the investor community have been criticised as being more interested in the next three months and not in company performance over the next year or more. Western Europe and Asia have been insulated from this trend to some degree as these markets are often characterised by controlling owners, including many families and industrial groups. Whatever a market's shareholding structure is, however, capital markets all benefit from shareholders who take more interest in the companies in which they invest: more interest in the performance of companies, in risk-taking, in board composition, in strategy, and in nearly all the issues this article has described. Yet shareholders are not always interested. They may not be interested because they wish to trade shares thousands of times a second—or they may not be interested because their business model makes them conflicted. In any case, it is becoming clearer, the further we travel away from the financial crisis, that effective corporate governance will require active owners, and certainly more active owners than we have seen to date. Whether and how this happens, it seems safe to say, remains one of the more intriguing and unknown factors in corporate governance over the next five to ten years.

Setting a higher bar for risk management

Global financial institutions increase risk management focus and resources

Edward Hida
Partner
Global Leader
Risk & Capital Management
Deloitte

David Merrill
Director
Deloitte

Heightened regulatory requirements and scrutiny of risk management and governance have led financial institutions to increase their risk management budgets and bolster their governance programmes, according to a recent global survey from Deloitte Touche Tohmatsu Limited. Deloitte's eighth biennial survey on risk management practices found that about two-thirds of financial institutions (65%) reported an increase in spending on risk management and compliance (up from 55% in 2010) to address rising risk concerns. The survey gathered data from Chief Risk Officers (CROs)—or their equivalents—at 86 financial institutions, including diversified financial services companies, banks, insurers and asset managers, with combined aggregate assets of more than US$18 trillion.

The majority of institutions that participated 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. This is not a trivial matter, as 39% of large institutions—particularly those based in North America—report having more than 250 full-time employees in their risk management function.

The survey's responses also illustrated divergence when it came to the spending patterns of institutions of different sizes. The largest and the most systemically important companies have had several years of regulatory scrutiny and continue to increase their focus on risk governance, risk reporting, capital adequacy and liquidity. In contrast, firms with assets of less than US$10 billion are now more likely to be concentrating on building capabilities to address what for them are a number of new regulatory requirements, which were applied first to the largest institutions and are now cascading downwards in the industry.

"The response to the financial downturn has led to far-reaching changes in financial institutions' risk management practices, with stricter regulatory requirements demanding more attention from management and increasing their overall risk management and compliance efforts", says Edward Hida, partner, Deloitte & Touche LLP and global leader, risk & capital management for DTTL and editor of the survey. *"That said, risk management shouldn't be viewed as only a regulatory burden or as a reporting exercise destined to gather dust on a shelf. Instead, it should be embedded in an institution's business framework, philosophy, and culture for managing risk exposures across the enterprise".*

The roles of management and the board in risk governance

The existence of a Chief Risk Officer (CRO) position at global financial institutions has grown steadily over the past eight years with the percentage of companies employing a CRO rising to 89% in 2012, up from 65% in 2002 and 86% in 2010. The current survey found that the CRO is a strategic, senior-level role at many financial institutions, reporting directly to the CEO or the board at nearly 80% of participating global financial institutions.

CROs are increasingly senior-level executives responsible for overseeing the risk management activities of their organisations who can advise the CEO and board on the organisation's risk profile and risk appetite. 87% of the institutions surveyed say the CRO assists in developing their organisation's risk appetite statement, while about 80% of CROs participate in executive sessions with the board or board risk committee and provide input into the development of business strategy. Some financial institutions have also created a chief compliance officer position, in some cases hiring former regulators to fill this senior-level opening.

Many financial institutions also report having a variety of management-level risk committees, such as asset liability management (74%), credit risk (59%), enterprise risk management (59%), operational risk management (44%), market risk management (44%) and investment risk (42%).

In addition, large institutions were more likely to have a variety of management risk committees, which is understandable because their activities and risk profiles are likely to be more complex. For example, 72% of large institutions report having a management-level operational risk management committee, compared with 43% of mid-sized institutions and 33% of small institutions.

Risk management has also risen significantly on the agendas of boardrooms. According to the survey, 94% of company boards now devote more time to risk management oversight than was true five years ago. In addition, 98% of company boards or board-level risk committees regularly review risk management reports, up from 85% in 2010.

Aligning incentive compensation and risk management

There has been extensive discussion about how some incentive compensation plans may inadvertently encourage excessive risk taking. Yet, only about half of the institutions, 49%, said that their board of directors reviews the compensation plan to consider the alignment of risks with rewards; this percentage increased in 2012 from 35% in 2010. Other actions related to compensation planning were reported more often: 83% of institutions said they use multiple incentive plan metrics, 73% require that a portion of the annual incentive be tied to overall corporate results, and 58% have deferred payouts linked to future performance. More institutions also reported using clawback provisions—41% in 2012, versus 26% in 2010.

One CRO who participated in the survey commented that a significant step in compensation plan development or change is approval by the risk function before the plan goes to the board. *"We have introduced what we call key risk takers, and when it comes to their annual assessment process, for every key risk taker there's mandatory input from at least one senior member of legal and compliance or risk in assessing that person's performance."*

Operational risk presents continuing challenges

According to the report, operational risk, which is a key component of the Basel II bank capital requirements, is a continuing challenge for institutions. Only 45% of firms rated themselves as extremely or very effective in this area, down slightly from 2010. These findings suggest that operational risk management capabilities are still developing, with many institutions implementing some of the basic steps to creating a programme. These steps include identifying risk types (completed by 81% of institutions) and gathering relevant data, such as key risk indicators and loss data (true for 60%). However, as was true in 2010, only about half of responding institutions had taken other necessary steps, such as standardising the documentation of processes and controls and developing methodologies to quantify risks.

Risk technology systems and data

As with the 2010 survey, the need for significant improvement in risk management technology and infrastructure was reported by many institutions. Less than one-quarter of institutions rated their systems as extremely effective or very effective in data management/maintenance, data process architecture/workflow logic, or data governance. The leading concern regarding risk technology continues to be the quality and management of risk data, where 40% of respondents were extremely or very concerned about capabilities at their own institution, followed by roughly one-third who said the same about the ability of their risk technology to adapt to changing regulatory requirements and the lack of integration among risk systems.

The highest priorities for new investment in risk technology systems were for improvements to risk data quality and management, cited by 63% in the current survey, versus 48% in 2010, and for enterprise-wide risk data-warehouse development, mentioned by 51% now, compared with 35% in 2010.

Other noteworthy findings from Deloitte's risk management survey

- Almost three out of four CROs rated their own institution to be either extremely or very effective in risk management overall, an increase from 66% in 2010's survey results
- The use of institution-wide enterprise risk management (ERM) programmes is continuing to grow. Today, 62% of financial institutions have an ERM strategy in place, up from 52% in 2010, while an additional 21% are currently building a programme. The total of 82% of firms that either have or are building an ERM programme is up significantly from 59% in 2008
- The impact of increased regulation is having a significant effect on business strategy and the bottom line, with 48% of firms confirming that they have adjusted product lines and/or business activities, a percentage that doubled from 24% in 2010

- Institutions are increasingly confident about their effectiveness in managing several specific risk types, including liquidity risk (85% rate themselves as extremely or very effective versus 77% in 2010); credit risk (83% against 71% in 2010); and country/sovereign risk (78% compared with 54% in 2010)
- Stress testing has become a central plank in many institutions' risk management efforts. 80% of the institutions surveyed state that stress-testing enables a forward-looking assessment of risk, and 70% say that it informs the setting of their risk tolerances

Key implications for management

As in past years, Deloitte's risk management survey examined a wide range of issues including governance, management of diverse risk types, methodologies, regulatory requirements and risk data and technology infrastructure. The findings from the current survey suggest a number of important issues that financial institutions should examine.

- **Managing regulatory change**
  The unrelenting pace of regulatory change is having a major impact on financial institutions through new requirements in many jurisdictions in areas such as regulatory capital, liquidity, restrictions on proprietary trading and the use of exchanges for most derivatives trades. There has been a particular focus on those institutions designated as systemically important, with requirements for higher capital levels, living wills and enhanced regulatory reporting, among others. The stricter regulatory requirements are demanding more attention from management, affecting the profitability of different lines of business, and increasing the costs of compliance. Financial institutions should consider how their business models will be affected by current and potential future new requirements, and whether their risk management programmes have the ability to respond flexibly to the ongoing process of regulatory change

Financial institutions may also consider their capabilities in stress testing macroeconomic variables and forecasting potential losses at the loan level

- **Strengthening governance**
  Given the strategic implications of risk management, it has become even more important that the board of directors and senior management provide strong leadership and promote a risk-aware culture throughout the organisation. The board of directors has the final responsibility for approving the organisation's risk policy and risk appetite, and for providing oversight of the risk management programme. Many financial institutions have also recognised the value provided by a CRO position—a senior-level executive responsible for overseeing the risk management activities of the organisation and who can advise the CEO and board of directors on the organisation's risk profile and risk appetite, the effectiveness of the risk management programme and the risk implications of strategic decisions

- **Examining incentive compensation**
  Ultimately, an institution's risk profile is the result of the many decisions made each day as employees seek to accomplish business objectives. Although the risk management function sets standards and provides oversight, employees in the business units are on the front line in terms of taking and managing risk. For this reason, institutions should consider reviewing their performance management and incentive compensation plans to ensure their alignment with the organisation's risk appetite

- **Managing a wider range of risk types**
  Institutions should consider whether they have sufficient capabilities to manage a wide range of risk types, in addition to more common risks such as market and credit risk. Developments in financial markets during the credit crisis raised the priority of managing liquidity risk. The pace of regulatory change has increased the importance of regulatory risk. Institutions are paying more attention to reputational risk given the potential for negative publicity and reputational damage if an institution fails to comply with regulatory requirements or becomes the target of an enforcement action. A varying series of management breakdowns at major financial institutions has also underscored the impact of operational risk events. Finally, many institutions are also giving a higher priority to managing model risk

- **Improving stress testing capabilities**
  The increased emphasis on stress testing for banks and certain systemically important financial institutions, especially among U.S. regulators, will require risk management programmes to have the capabilities to employ this technique on scenarios stipulated by their regulators as well as on their own scenarios. An effective stress testing programme requires governance structures and controls to oversee data integrity, the selection of stress testing models and model validation. Financial institutions may also consider their capabilities in stress testing macroeconomic variables and forecasting potential losses at the loan level. When stress testing is used to assess capital adequacy, institutions should consider whether it is part of a broad, well-documented internal capital adequacy assessment process

- **Upgrading risk data quality and technology infrastructure**
  Managing risk effectively requires institutions to be able to aggregate and analyse risks on a consistent basis across the organisation in order to provide timely reporting to management and regulatory authorities. Institutions should consider whether they may need to improve the quality and consistency of risk data and also upgrade their risk technology systems in order to gain such an enterprise-wide view of risk

The unsettled market and economic conditions of the last several years have created a new and dynamic environment for financial services. Governments and regulatory authorities responded by introducing major regulatory reforms intended to strengthen the financial system, in large part by seeking to increase the likelihood that individual institutions will have sufficient capital and liquidity to survive a future crisis. As they respond to regulatory and other market and competitive challenges, financial institutions will need to continue to enhance their risk management capabilities—setting a higher bar.

Access the complete report of findings from Deloitte's **'Global Risk Management Survey',** eighth edition, at www.deloitte.com/us/globalrisksurvey.

Institutions are paying more attention to reputational risk given the potential for negative publicity and reputational damage if an institution fails to comply with regulatory requirements or becomes the target of an enforcement action

Governance, Risk and Compliance (GRC) software
Business needs and market trends

David Cau
Director
Business Risk
Deloitte

The importance of a holistic view of risk and compliance issues and the difficulty to achieve it is often recognised as a weakness for many organisations. As an indication that significant improvements may be required at many organisations, the recent Deloitte Global risk management survey (eighth edition) reveals that when asked about their capabilities of their data strategy and infrastructure, no more than one-third rated them as extremely or very effective in any area.

As an organisation progresses in developing its risk management, internal audit and compliance practices, the issue of investing in an automated solution to improve efficiency will arise sooner or later.

Tools for governance, risk and compliance functions

First of all, it is important to clarify the concept of GRC. Although various definitions do exist, the definition proposed by Nicolas Racz, Edgar Weippl and Andreas Seufert in their recent research paper 'Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)' provides a rather comprehensive view of the concept. In this paper, GRC is defined as "*an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness*".

The primary purpose of GRC software is therefore to automate much of the work associated with the documentation and reporting of the risk management and compliance activities that are most closely associated with corporate governance and business objectives. The primary end users include internal auditors and the audit committees, risk and compliance managers, and accountable executives. The key functions of GRC software are usually the following:

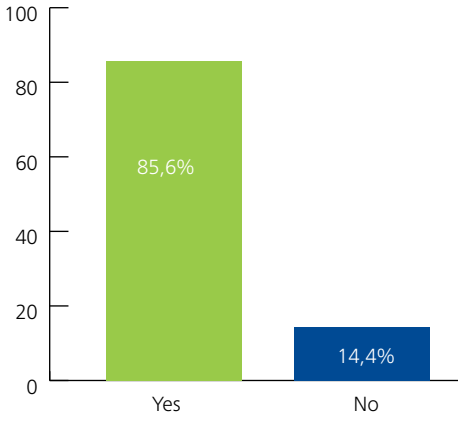
- Audit management functions that support internal auditors in managing work papers, and scheduling audit-related tasks, time management and reporting
- Policy management features that include a specialised form of document management that enables the policy life cycle from creation to review, change and archiving of policies; mapping of policies to mandates and business objectives in one direction, and risks and controls in another, as well as the distribution to and attestation by employees and business partners

- Compliance management functions that support compliance professionals with the documentation, workflow, reporting and visualisation of control objectives, controls and associated risks, surveys and self-assessments, testing and remediation. At a minimum, compliance management will not only include financial reporting compliance (e.g. SOX compliance), but can also support other types of compliance, such as industry specific regulation (e.g. ISO 9000) and compliance with internal policies
- Risk management functions that support risk management professionals with the documentation workflow assessment and analysis reporting visualisation and remediation of risks (as defined in ISO31000). This component focuses generally on risks and incidents follow-up but may also collect data from risk analytics tools (Credit Risk, Market Risk, etc.) to provide a consolidated view of risks

The GRC software market: the business need

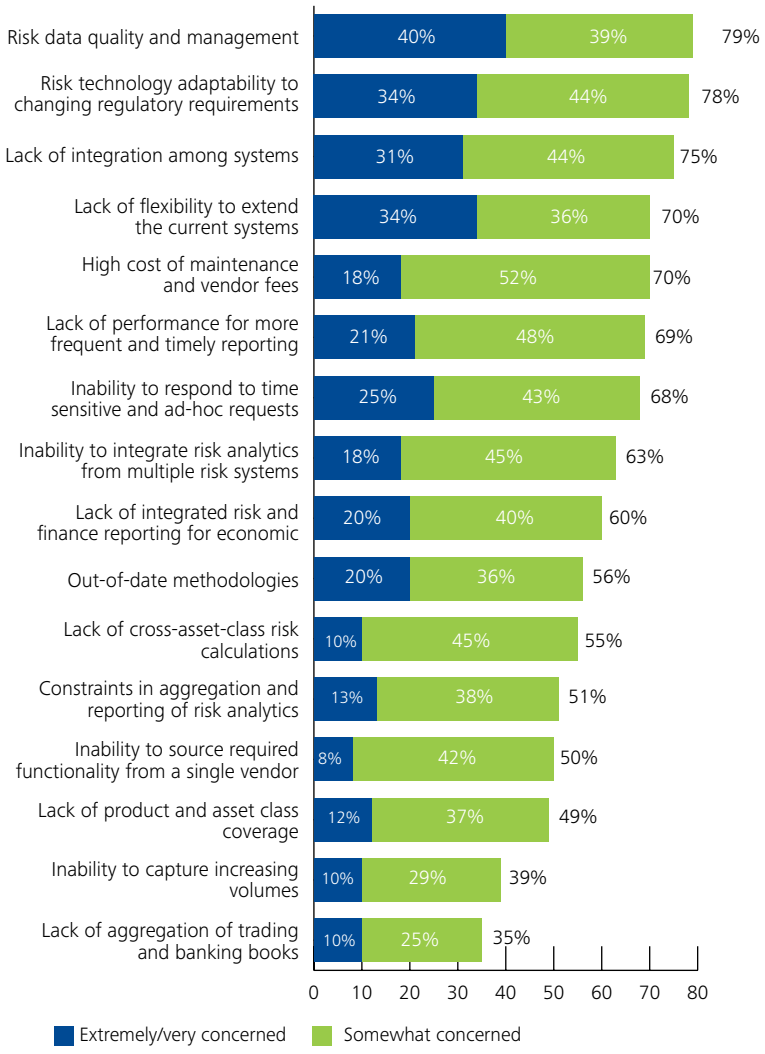
- Most organisations are aware of the need for a significant improvement in the way they manage their risk, internal audit and compliance functions through better automation of data and information. As illustrated by an OCEG survey, 85% of companies interviewed are convinced that they would benefit from integrating the use of technology for their GRC activities. The need for a GRC technological solution is there, but the question remains: which technological tools will be able to provide the appropriate solution?
- In the eighth edition of the 'Deloitte Global Risk Management Survey', organisations cited a number of concerns about their risk management information technology systems (Figure 2)
- Among the main concerns addressed, the ability of organisations to easily upgrade or revise their systems risk technology, 78% of companies are extremely, very or somewhat concerned about their ability to adapt to changing regulatory requirements, as well as the lack of flexibility to extend the current systems. Related to this issue, 75% of organisations are extremely, very or somewhat concerned about a lack of integration among systems and 63% of the organisations have issues with an inability to integrate risk analytics from multiple risk systems. Many organisations maintain different information systems for specific products or geographies, sometimes due to past acquisitions, and it can be difficult and expensive to combine their output or else to replace them with an integrated information system
- Moreover, the pace of regulatory change has put the emphasis on the ability of organisations to have risk systems that can respond quickly to new requirements. This appears to be a concern especially for larger institutions: 40% of large institutions said they were extremely or very concerned about the ability of their risk technology to respond to new regulatory requirements, as did 44% of mid-size institutions and only 12% of small institutions
- Some of the other top priorities for investment include risk analytics and risk reporting: risk analytics (53%), real-time risk monitoring (51%) and risk dashboards (44%)
- But the fastest growing business need relates to risk data quality and management, with 79 % of institutions at least somewhat concerned, including 40% who are extremely or very concerned. Creating consistent data standards is a challenge for organisations, which often source data from multiple locations with incompatible data formats. Further, departments within an organisation may not realise that they both have a relationship with the same counterparty as each may do business with a different business unit or subsidiary

Figure 1: Would your organisation benefit from integrating and streamlinning use of technology for GRC activities enterprise-wide?



The need for a GRC technological solution is there, but the question remains: which technological tools will be able to provide the appropriate solution?

Figure 2: How concerned is your organisation about each of the following issues for its risk management information technology systems?



The GRC software market: the offering

Market overview

The GRC market as defined by the technology industry is about 10 years old, and buyers have high expectations for the performance of GRC software.

Up to now, from a technical perspective, organisations have generally opted for risk management systems installed in-house, whether developed internally or by vendors, rather than hosted externally. Indeed, according to a recent Deloitte survey, roughly 40% of organisations said they were likely to make a major investment over the next 12 months. Among these organisations, 45% were considering internally-developed applications, while 41% would rather opt for third-party vendor applications installed in-house (41%). Third-party vendor applications hosted by a vendor (20%) were cited less often as a target for major investment. Data privacy concerns around confidential information being hosted off-site may well be a reason this last approach seems to be adopted less often.

The GRC software market is dominated by key players like IBM, RSA Archer, Thomson Reuters, SAP or Oracle. Deloitte has established strong strategic and technical alliances with these key players in order to better serve the clients that have opted for these softwares. But the market is still offering a significant place to niche players (e.g. MetricStream, Sword, Checkpoint, Mega and Aris). Moreover, the GRC market seems to be thriving, as more companies realise that they pretty much have to invest in this area, and so the market landscape might rapidly evolve as a result.

It is important to mention that this market segmentation is more a question of size of vendor rather than a significant price differentiation. Price is key, as sometimes the business case for GRC software is often strongly questioned and budgets for GRC software are often limited in most of the companies and licence fees or, more globally, the Total Cost of Ownership (TCO), namely the cost of development, implementation, licence fees and maintenance of a GRC solution is usually similar.

Most of the recent market studies forecast an annual rate of increase of 10% over four years. Indeed toward the end of 2011, after the market had grown 18% in 2010, Forrester Research data suggested a CAGR of 14% or so through 2015. TechNavio, for its part, has recently forecast that the Global GRC software market will grow at a CAGR of 9.2% over the period 2012-2016, driven by *"increasing demand for comprehensive solutions"*, which seems to favour the biggest players in the industry, such as EMC, IBM, Thomson Reuters and the big ERP players (SAP and Oracle), though it is worth mentioning that projected growth rates in previous years have been even higher.

A strong consolidation, with a shift from best-of-breed players to well-established vendors will also be a key market trend. This consolidation trend will be driven by the need for greater investment in complex risk analytics to face the 'big data' problem of the vast majority of organisations.

Differentiation today is also about the ability to deliver against multiple use cases, and provide advanced risk management functionality, with analysis of the impact of risks on strategic objectives and business performance, domain expertise in multiple highly regulated industries, ease of use—including mobile capabilities—and configurability.

GRC software market view in Luxembourg

The GRC software market is still emerging in Luxembourg, but the situation is rapidly evolving and differs among sectors.

In Luxembourg the banking sector is already well equipped with various niche solutions covering one specific aspect of risk (market risk, credit risk, operational risk, liquidity risk) and compliance. This sector is facing the issue of a lack of integration of its various solutions and has difficulty in migrating or integrating the various applications into an overarching structure. However, the recent CSSF circular 12/552 is already contributing to the development of the GRC market as this new regulation recommends more and more efforts on common governance on risk and compliance issues.

Investment management, a key sector in Luxembourg, is up to now significantly underequipped with GRC software. The main reason seems that investment management sector is highly fragmented with various actors, who are still overwhelmed by the operational management/set up of regulations, such as AIFMD or EMIR. Moreover, it has to be said that the vast majority of GRC players is not offering the appropriate solutions to this sector: both pricing models and key features proposed by GRC vendors are not yet fully adapted to this market.

The insurance sector is increasingly interested in GRC solutions, but either local players are part of international groups and have to use (or wait for) the corporate solution or they are small and cost is often perceived as a key hindrance for a the implementation of a GRC software.

The industry and public sector is increasingly ready and interested in GRC software and is generally starting its GRC project with the implementation of an operational risk application/module. New regulations such as REACH, CLP or quality-related recommendations are also pushing the industrial sector to enhance its holistic approach of risk, internal audit and compliance.

Key trends affecting the GRC software market

The functions of GRC software are evolving on the basis of several trends, which include:

- A growing need for internal audit features as organisations face increasing regulatory requirements, GRC oversight and demands for more business performance audits
- An increasing need for regulatory content services and change management to deal with regulatory proliferation. In the aftermath of the 2008 global financial crisis, GRC has to support the transparency objectives of regulators and decision making by business leaders. Currently the regulatory focus of the software is on anti-corruption and bribery
- The development of risk analytics to support integration of risk management and performance management
- The emergence of third-party risk management to ensure that third parties do not present unacceptable compliance and risk
- A focus on operational technology and critical infrastructure protection, which increases the variety and volume of risk and control data ('big data' management)

Moreover, the GRC market seems to be thriving, as more companies realise that they pretty much have to invest in this area, and so the market landscape might rapidly evolve as a result

GRC software selection

Usual approach: vendor selection based on 'quadrants'

Most companies that are opting for third-party GRC software tend to base their GRC software selection on GRC market 'quadrants' analysis, mostly performed by Gartner and Forrester. Instead of simply showing statistics or ranking companies in lists, GRC market 'quadrants' use a two-dimensional matrix to illustrate the strengths and differences between vendors.

The most common criteria used by these quadrants are the ability to deliver GRC functions (audit management, compliance management, policy management and risk management) and a credible presence in the marketplace (an existing enterprise GRC client base, a growth strategy and brand, support capabilities, a strategy for and investment in continued innovation in GRC solutions and related products, geographical reach and financial strength).

However, these quadrants may lead companies to limit their GRC tool selection process only to the vendors mentioned in the quadrants, or even only consider players from the leader's quadrant and initiate their choice only from an IT standpoint, rather than also considering the business needs.

Deloitte holistic approach

The key driver for the holistic approach of a GRC software selection process is the agnostic position of Deloitte regarding technological solutions.

The main purpose is to find the solution that gives the best value for money for clients. Deloitte uses a well-proven methodology that will guide the client through the evaluation process for software options, allowing the client to make a decision based on a sound analysis. The selection process generally encompasses seven phases (as illustrated in figure 3).

It will be important to start a GRC selection project with a deep analysis of the client's business needs and context in order to formalise the functional coverage. Then, a clear view on the client's current IT environment (existing specialised solutions or enterprise solutions—ERP) has to be obtained. These analyses will help to see if the best option will consist in developing a new solution internally, buying a packaged solution or opting for a best-of-breed solution. These reviews will also enable to evaluate if, given the current situation, the implementation is realistic.

If the best option identified consists in the implementation of a third-party/vendor solution, it will be necessary to see how we can identify the best solution on the market from the wide range of software currently available. Five key areas of criteria will enable to select a list of potential candidates that will be able to make live demo (based on specific client requirements). Lastly, price negotiations and final technical adjustments discussions will come into play in order to select the target solution.

Deloitte's specialists will therefore help clients throughout their selection process, providing specific support when it comes to performing an analysis of requirements, and helping to draft calls for tender, conducting research on the software market and offering a selection of appropriate suppliers or making the final decision through coaching, support and analysis.

In a nutshell, integration is the key idea regarding the current and future situation of GRC software. There is a need for integration of the decision process within the organisations. Too often, decisions concerning GRC technical solutions are taken at department level and only cover a specific aspect of the GRC spectrum. There is a need for technical integration, as most of the companies have to deal with existing solutions. There is also a trend for integration among the GRC solution providers, driven by the need for greater investment in complex risk analytics to face the 'big data' problem of the vast majority of the organisations. In fact the need for integration is rather logical as it is the essence of GRC itself.

Figure 3

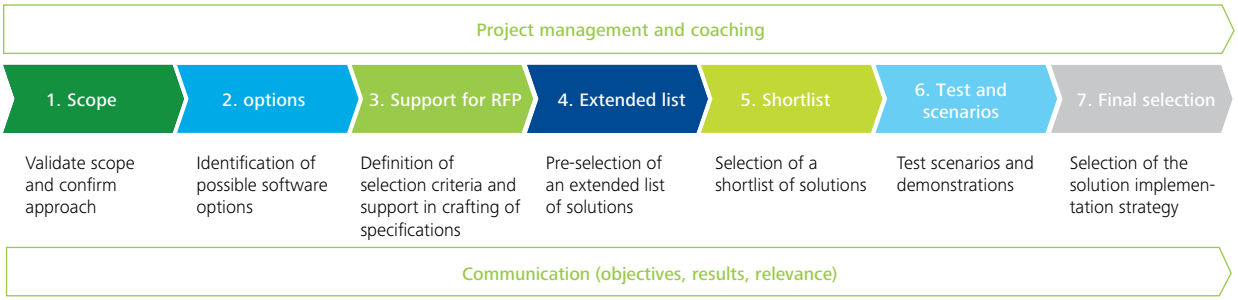


Figure 4

1. Functional coverage

- Are the answers regarding specific functions clear or are they deliberately vague?
- Functional coverage is not perfectly matching with the expectations

2. Technical architecture

- Is the software available in multiple versions for multiple environments (Windows, Linux, Unix, etc.)?
  This demonstrates the suppliers's experience working in various technical environments
- Is the solution modular?
  This will facilitate further development (sustainability)

3. User friendliness

- Design of screens
- Predictive text input
- Number of entries required for the operation
- Level of customisation of reports

4. Costs

- Is the implementation of the solution clearly described (e.g integration of existing data, time required for setup, time and cost required for the customisation of the solution)?
- Is the cost of consultants that will implement the solution clear (fixed price? travel costs?)?
- Is the cost of licenses clearly defined?
- What does the maintenance contract exactly cover?

5. Vendor characteristics

- Has the vendor replied in a timely manner? This is a measure of the seriousness of the supplier and available resources
- Does the vendor understand the requirements?
- Are the vendor references comparable? Some vendors have many references... in other continents... or other products.
- Is the vendor a 'market maker' or a 'market follower'?

The pith and marrow of risk appetite[1]

Jean-Philippe Peters
Director
Business Risk
Deloitte

Many financial institutions are paying a lot of attention these days to the design and implementation of an adequate system of internal risk governance, which includes responses to challenges such as:

- Structuring the three lines of defence and articulating the role of the internal control functions (risk management, compliance and internal audit)
- Ensuring adequate risk oversight by senior management through enhanced risk-based MIS capabilities and related data analytics, further embedding of risk factors in the decision-making process or on-going education and training
- Developing capital planning capabilities and projecting overall solvency over the business plan horizon
- Defining risk appetite and translating it into operational limits

This article focuses on the last item in this list by clarifying key concepts and addressing the main practical challenges for companies that have embarked on the definition of their risk appetite.

There are both 'push' and 'pull' arguments for firms to improve their risk appetite frameworks. The 'push' arguments come from the slew of recent or forthcoming regulation and supervisory guidance that will compel firms to improve the way that their risk appetite frameworks operate—or in some case build this capability from scratch. The regulatory landscape for banking and insurance firms—be it speeches, working papers and draft or final regulation—is indeed full of references to risk appetite, its benefits, uses, applications and case studies of failed firms whose weak risk appetite frameworks played a part in their downfall. When firms are criticised for shortcomings in their risk governance and management, an appetite framework is commonly prescribed as a cure by regulators. And yet, there remain a surprising variety of opinions about what it actually means to establish and embed a proper risk appetite framework.

Risk appetite limits are thus about putting individual risk-taking in a strategic and firm-wide context and perspective

Just as importantly, however, the 'pull' arguments come from the firm-wide benefits that accrue once risk appetite is properly embedded within an organisation: conscious risk taking, joined-up risk management or specific focus on the drivers of quality risk management can all be valid drivers for establishing a sound risk appetite framework.

From risk appetite to risk tolerance

Before delving into some of the practicalities of defining and designing a Risk Appetite Statement (RAS), let us clarify some critical concepts used throughout this article:

Risk capacity: *the maximum level of risk at which a firm can operate, while remaining within constraints implied by capital and funding needs and its obligations to stakeholders.*

No firm should want to operate at its capacity, since there would be a very real risk of a breach. Once the capacity has been understood, a crucial task of risk management is to understand how a firm's activities expose it to risks that use up that capacity. While capacity can be expressed in terms of available own funds or liquidity, the obligations the firm has to its stakeholders—be they the ultimate owners of the firm, its customers or regulators—are the constraints that can be used to define capacity.

In other words, this is the maximum amount of risk the company is able to assume and therefore represents the upper boundary for the risk appetite.

1 This article contains extracts from Deloitte's white paper 'Risk appetite frameworks: How to spot the genuine article' published by our EMEA Centre for Regulatory Strategy and from the article 'Risk Appetite: More than a Catch Phrase' by Thierry Flamand and Jean-Philippe Peters (Deloitte Luxembourg), released in PRiM Risk Newsletter No. 30, July 2012.

***Risk profile**: the firm's entire risk landscape reflecting the nature and scale of its risk exposures aggregated within and across each relevant risk category.*

We think it is important to emphasise that the true risk profile of a firm can never be known in full. It's a multi-dimensional set of sensitivities to a wide range of potential risk drivers. But the profile can be estimated by pertinent, timely and accurate assessments of a firm's exposure to risks, taken from many complementary perspectives—including concentration risk, wrong-way risk and correlations across risk types or scenarios. Furthermore, knowing the likely shape of risk exposures through the cycle can be equally or even more important than knowing it for a particular point in time.

***Risk appetite:** the risk a firm is willing to take in the pursuit of its strategy.*

The crucial features of this definition are: 'willing', which denotes a conscious recognition and acceptance of the risk/return trade-off; 'pursuit', which acknowledges that firms may fail to achieve their goals, while still bearing the risk; and 'strategy' which highlights how appetite should always be considered in light of the firm's overall business model.

The articulation of risk appetite in written form is the Risk Appetite Statement (RAS).

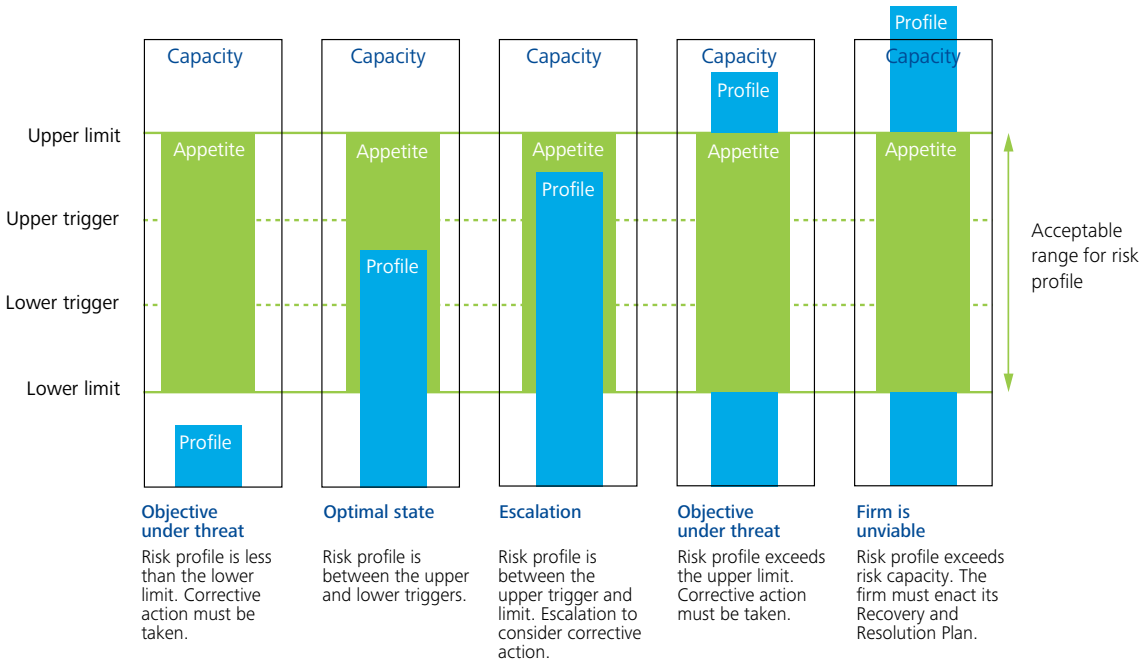
***Risk tolerance:** the level of risk which, if breached by the firm's risk profile, would necessitate immediate escalation and corrective action.*

The risk appetite is drilled down through allocation of risk tolerance and target levels for the many constituents composing the organisation's risk profile. It is translated into measurable and tractable limits that trigger actions in the event of breach.

Risk appetite limits are thus about putting individual risk-taking in a strategic and firm-wide context and perspective. Risk appetite limits can be set up to provide both a floor and a ceiling on risk taking, or just to provide a ceiling. In the firms and countries where risk appetite frameworks are moving to encompass strategic and business risks, limits are more likely to be calibrated in terms of a both a floor and a ceiling.

These concepts of risk appetite, capacity, statement, limit and trigger combine to form a coherent way of understanding and communicating risk taking within firms, as shown below.

When associating these various concepts in practice, monitoring of the firm's risk profile against appetite can be implemented and various situations can arise, as illustrated in the graph below.



From theory to reality: challenges and pitfalls when implementing a risk appetite framework

Practical usage of the theoretical concepts introduced in the previous section can often be a daunting task in many organisations, as the process of setting up a framework can be complex and time-consuming, and will depend on the nature and complexity of the firm. It can be tempting for a firm facing huge amounts of regulatory and strategic changes to take a short-cut with risk appetite.

Most financial institutions will already have a large number of limits in place, be they credit, market or liquidity limits. Faced with pressure to demonstrate progress on the risk appetite front, it is relatively easy for a firm to take existing limits and relabel, rebadge or repackage them for approval by the Board as a fully-fledged risk appetite framework. After all, isn't risk appetite just a set of limits put together?

Unfortunately (or fortunately should we say) not: only if risk limits are the expression of a firm-wide process of articulation (meshing top-down direction from the Board with bottom-up communication of risk insight) will they help to link the firm's overall strategic plan with its risk strategy, its risk management and its actual risk taking. The golden rule when initiating such a process is to bear in mind this fundamental principle: risk appetite statements should reflect a risk-taking behaviour that is aligned with business objectives and is specific to the company and its strategy. If limits are not calibrated as part of a shared, firm-specific risk appetite language then individual limits may be largely irrelevant: an isolated limit set outside of a firm-wide strategy may fail to protect it because there is no overall logic to its calibration.

We therefore believe that a well-sequenced and structured approach can help demystify the risk appetite concept while offering value-adding perspective to governing bodies on how their institution actually conduct risk taking activities.

So, how do you set the tone at the top and then roll-out the Board's risk strategy as operational limits? And what should you pay attention to?

A **first commonly observed pitfall** is restricting the approach to the overall regulatory solvency ratio (Pillar I) by fixing a target ratio and allocating maximum capital requirements by major risk types. The exercise can then become cumbersome and resulting limits are difficult to pilot from an operational point of view. While solvency is of course critical in assessing the overall risk profile of a company, it should actually be completed by other business indicators used by senior management in its decision-making process. This enables easier communication to governing bodies (including the board of directors) and better embedding of limits in day-to-day management.

What a risk appetite framework does is to extend this approach to all of a firm's risks—and work out the linkages between those risks, its overall strategy and the lower-level risk drivers of its risk profile. Capturing the breadth of risk taking is central to a good framework.

For example, a financial institution will take on data quality risk whether it likes it or not. A standard (and self-defeating) approach to this risk is to exclude it from the appetite framework, and to focus instead on financial risks, which are more readily measurable. But a risk appetite framework will encourage the business, the Board and risk managers to ask difficult questions and find ways to assess the expected and the stressed risk position. It is better to have an approximate measure of data quality risk, and an awareness of where it is most likely to hurt you, than no idea at all.

Furthermore, any redesign of the business model may raise or reduce data quality risks and these changes in the risk profile should be made in a conscious, well-informed fashion. Once data quality becomes part of the landscape of risk appetite and risk measurement, top-down direction can be given by the Board, and bottom-up assessments of the business or control environments can be developed.

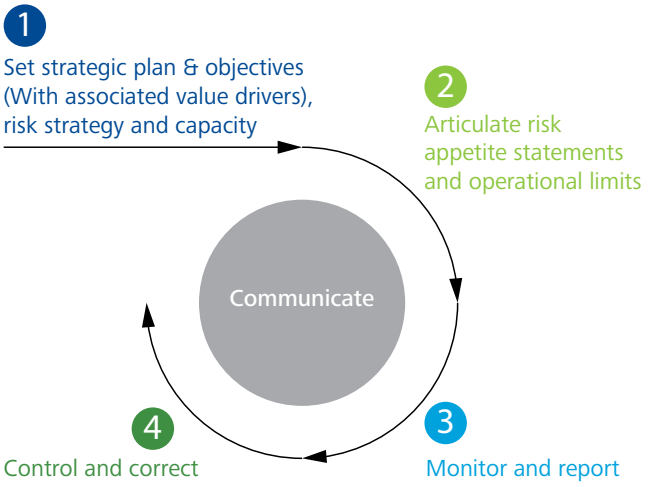
A second pitfall relates to the false belief that a RAS should necessarily require advance modelling tools to be fixed and monitored. In a similar way to other aspects of the second pillar, the principle of proportionality applies to methods and metrics used for risk appetite as well; it does not, however, exempt a company from defining and formalising the RAS!

For many small and/or non-complex players, a pragmatic approach to this problem makes full sense and existing material should be leveraged as much as possible. More specifically, strategic plans are accompanied by a handful of quantitative and qualitative statements that serve as drivers for developing business projections. This might include, for instance, minimum dividend yield to distribute to shareholders, a focus on reputation and compliance, growth in net assets under management (or underwritten premiums), cost-income ratio, etc. These targets and objectives should serve as the starting point for delimiting the company's risk tolerance by setting related operational limits.

A useful approach for deriving the risk appetite statement in practice is to combine this top-down view with a bottom-up analysis and ensure both converge. More precisely, senior management could derive a limited number of metrics (say, 4 to 6) associated with its strategic objectives over the business plan horizon and define limits, thresholds or targets for each of them. In parallel, existing operational limits (e.g., investment guidelines, product or geographical restrictions, duration gap between assets and liabilities) should be identified and listed. Both views are then compared and reconciled to ensure the operational limits contribute to meet the strategic objectives (and associated limits).

As illustrated in the figure below, this process should be seen as iterative: supervisory authorities do not expect all financial institutions to develop a fully embedded and self-functioning risk appetite framework from day 1. A stepwise approach with a period of testing, especially for the adequacy of the limits, is more likely to be adopted. Setting limits at the appropriate levels to ensure that they fit the purpose is indeed one of the key challenges faced by financial institutions. Limits should act as a warning sign before it is too late and the red alarm should not be activated at untimely moments. The right balance is not always easy to reach and the robustness of their value should be monitored and tested over time.

A stepwise approach with a period of testing, especially for the adequacy of the limits, is more likely to be adopted

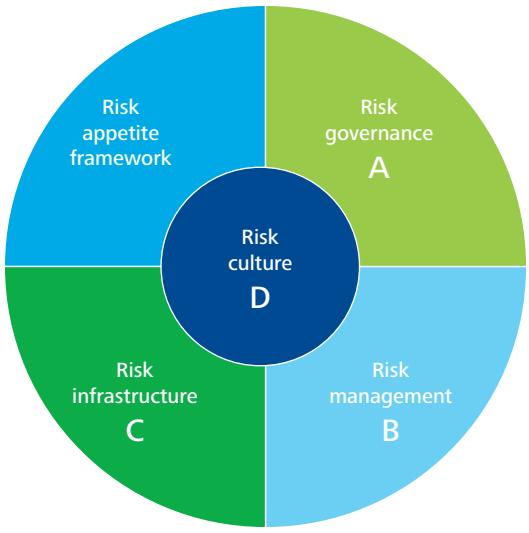


Another challenge encountered by financial companies when developing a risk appetite framework is that current operational limits are inherited from past situations that do not necessarily reflect the actual risk tolerance seen as acceptable by senior management. Existing limit systems are often established on 'market practices' (e.g., maximum net FX open position), 'gut feeling' and 'expert knowledge' (e.g., maximum duration gap, issuer concentration, etc.), leading to inconsistency between actual and expected risk exposure. This highlights the importance of proper reconciliation between strategy-driven dimensions (top-down) and existing operational limits (bottom up) in the process illustrated above (see in particular step 4).

As will be clear by now, a risk appetite framework is not just another risk management tool operated in isolation by the risk management function. Making risk appetite work for an organisation implies well-considered change to four interlocking and mutually reinforcing elements: the risk appetite framework itself, its risk governance, the associated risk infrastructure, and its suite of risk management tools.

However, as illustrated in the figure, central to a firm's risk management and governance must be its risk culture. A firm's risk management needs to respond to its business and risk strategy and how it positions itself in markets. The risk appetite framework provides the key way to link a firm's strategy and its management of risk.

Once properly integrated, a firm's risk appetite framework will both support and be supported by: (A) its risk governance, (B) its risk management tools, (C) its risk infrastructure, and (D) its risk culture. The linkages are explained in more detail on the following page.



	How the firm's risk appetite framework provides support	How the firm's risk appetite framework is supported
A	The risk appetite framework and language support **risk governance** by providing the Board and senior management with the information and tools needed to understand and communicate the risks the firm is and should be taking in line with its risk appetite and its business and risk strategy.	The firm's **risk governance** is essential to ensure that lines of accountability exist and staff adhere to the firm's risk appetite framework. Implementation and running of the risk appetite framework depend crucially upon the full buy-in of Board and senior management and the tone at the top.
B	The risk appetite framework supports the firm's wider **risk management tools**. It provides information to support the efficient use and development of the firm's risk management tools.	The firm's wider **risk management tools** support the risk appetite framework. For example, running stress tests aligned to the firm's targeted future risk profile and its business and risk strategy supports the firm's calibration of its risk appetite and limits.
C	The firm's **risk infrastructure** (including timely aggregation and reporting of risk data, related systems and processes, and employee skillset) must respond to and support its current and targeted future risk profile and its business and risk strategy. The risk appetite framework identifies comprehensive, firm-wide information necessary to shape the firm's risk infrastructure.	A robust and well developed **risk infrastructure** responding to the firm's current and targeted future risk profile and its business and risk strategy is essential for its risk appetite framework. It is a prerequisite for effective monitoring, reporting and control of risk appetite, profile and capacity.
D	The risk appetite framework and language inform a strengthened **risk culture** grounded in the shared value and common practice of understanding, clearly communicating, and controlling how each employee's activities contribute to the firm's risk profile and the successful implementation of its strategy.	A firm's **risk culture** is in its language and the style and quality of its internal communication. It is instrumental in the full operational embedding of the risk appetite framework since only the firm's risk culture helped by the tone at the top and appropriate compensation can turn risk appetite statements and limits into a risk appetite language that is spoken and understood throughout the firm.

Conclusion

Risk appetite is a measure of the risks that an organisation is willing to accept in pursuit of its objectives. As such, it should not be limited to solvency considerations. The various aspects of the company's strategy should be reflected in the framework (including both qualitative and quantitative elements). It should lead to the definition of meaningful and practical risk limits that can be understood on the 'shop floor' and rolled up to board level, as this is the best way to embed high-quality risk management across the organisation.

The proportionality principle does not exempt companies from formalising their risk appetite statement so that all financial institutions should consider embarking on the risk appetite journey. The process of defining and calibrating the framework and the associated metrics needs time to mature, but pragmatic approaches can be defined to enable companies to harvest the fruits of the process.

An important success factor is thus to identify the key risks to delivering the strategy set in the business plan and make sure operational limits in place adequately reflect this view. Alignment is indeed often needed as historical limit systems have been gradually built in silos and lack consistency.

While not a straightforward exercise to perform, adopting a structured risk appetite aligned with business objectives is the heart of the matter here, as it can deliver value to companies of all size and complexity by:

- Striking a better balance between risk and reward (and hence creating value)
- Enhancing overall communication of governing bodies to stakeholders (regulatory, shareholders, business units) about their expectations
- Enabling the development of a business culture with a high awareness of risk

Risk management within AIFMD for private equity and real estate funds

Xavier Zaegel
Partner
Capital Markets/Financial Risk
Deloitte

Sylvain Crépin
Senior Manager
Capital Markets/Financial Risk
Deloitte

Jean-Maxime Pradelle
Analyst
Capital Markets/Financial Risk
Deloitte

In a nutshell

- The AIFMD framework marks a major development for private equity and real estate funds with regard to risk management requirements
- The interpretation and implementation of these requirements raises a number of questions and challenges in relation to governance, roles and responsibilities and risk measurement techniques
- Identification and close monitoring of risks in private equity and real estate investments require specific expertise and expert judgment which cannot be expressed through the quantitative risk indicators commonly used in more traditional financial asset classes
- A meaningful and appropriate risk monitoring and reporting process can increase transparency and disclosure for the ultimate benefit of investors and AIFMs, turning client servicing into asset growth

Introduction

The Law of 12 July 2013 implementing the Alternative Investment Fund Managers Directive (AIFMD) in Luxembourg and the EU Commission Delegated Regulation 231/2013 (Level 2 Regulation) set up the new regulatory framework for Alternative Investment Fund (AIF) risk management, with many of the implementing measures and authorisation processes now in place. While compliance gaps for AIFM already in line with UCITS regulations have proved to be limited (with the notable exception of regulatory reporting, remuneration and risk management of illiquid assets), compliance may be more challenging for pure alternative players such as private equity, infrastructure and real estate managers, for which most of the AIFMD requirements, are completely new.

Among the challenges faced, risk management requirements for private equity and real estate raise many questions and concerns within the industry, along with regulatory reporting, which is characterised by risk metrics and risk-related data. Identifying and implementing appropriate risk measurement techniques and procedures for those very specific asset classes is likely to represent a challenge for risk managers, on top of the organisational and independence requirements relating to risk management.

This paper aims to present in detail the challenges faced by private equity and real estate managers in meeting AIFMD risk management requirements and the potential solutions available going forward. It is structured in three parts: governance and organisation (strategic level), risk identification, measurement and documentation (tactical level) as well as risk monitoring and reporting (operational level).

Governance and organisation

Organisation

Most private equity and real estate managers have to adapt their organisation to incorporate a permanent risk management function that in most cases did not exist at the time of AIFMD implementation. This function should have full escalation and whistleblowing capacity with respect to the governing body, while being hierarchically and functionally independent from portfolio management activities. Defining an independent line of reporting may involve strategic reshaping of the organisation to ensure the independence of risk management up to the governing body of the AIFM. Possible solutions include recruitment and the merger or outsourcing of functions, all of which present pros and cons.

Recruiting an experienced risk manager with appropriate industry specialisation offers significant benefits, as he will be able to provide insightful support in setting up the function and ensuring compliance with independence and ongoing risk monitoring and management requirements without an additional workload being created. However, appropriate profiles in the market might limit this solution to a small number of players.

Combining risk management with the compliance function on the basis of the proportionality principle, if approved by the regulator, has the obvious advantage of not incurring extra costs. Training and delegation of certain aspects may be required in case of lack of time or experience.

Outsourcing part or all of the risk management function is the last option. The AIFMD regulatory framework defines the extent of delegation for the portfolio management and risk management functions. As it is clearly aimed at avoiding 'letter box' entities, the substance of the management companies will be in the spotlight. Outsourcing will have to be carefully analysed as outsourced activities should not exceed by a substantial margin the functions performed by the AIFM itself.

Roles and responsibilities

Once created, the roles and responsibilities of the risk management function should be clearly stated. The minimum regulatory requirements are:

- The implementation of effective risk and liquidity risk management policies and procedures in order to identify, measure, manage and monitor on an ongoing basis all risks to which each AIF is or may be exposed, including through the use of stress tests
- The monitoring of the risk profile of each AIF and its compliance with the risk limits set in accordance with Article 44 of the AIFM Regulation
- The notification in a timely manner to the senior management of the AIFM when it considers that the AIF's risk profile is inconsistent with these limits or sees a material risk that the risk profile will become inconsistent with these limits
- The provision of regular updates to the senior management of the AIFM, outlining the current level of risk to which each managed AIF is exposed and any actual or foreseeable breaches of any set risk limits, the results of stress tests and scenario analyses

To achieve these objectives, the risk manager could benefit from close interaction with other functions (i.e. portfolio management, valuation, internal audit and compliance) and from their specific expertise. The monitoring of investment risks and the various risk analyses performed by portfolio managers and the valuation function could serve as very good basis for the risk management function to be reviewed and challenged, and complemented where necessary with additional independent analyses. Despite relying partially on other functions' output, the risk manager should cover the whole risk management cycle that encompasses pre-investment risk, risk measurement, risk monitoring, stress testing and reporting.

In order to formalise and organise the risk manager's roles and activities, it is necessary to define a comprehensive job description detailing activities as well as the content, frequency and recipients of reports .

Risk identification and measurement

Risk management policy

The risk management function has to operate based on written procedures, with the risk management policy being the core document detailing its structure and operations in terms of risk governance, risk profiling, risk limits, risk measurement and monitoring techniques as well as risk reporting content and frequencies. The risk management policy should be carefully prepared, as it will be scrutinised by the regulator as part of the authorisation process, and will be periodically reviewed.

Risk identification

Unlike vanilla asset classes such as listed equities and fixed income securities, private equity and real estate investment funds have a limited risk management culture, with most of the investment and risk management expertise being concentrated at the level of the portfolio management team. The key role of the risk manager is to identify all the risks that the managed AIFs are, or might be exposed to, and to assess their significance. Common risks faced by private equity and real estate funds relate to funding, financing, concentration, valuation, key people, governance, etc. Some risks may be related to the nature of the investments, with a direct or indirect impact on their valuation, while others may affect the portfolio or the fund only. The regulator has clearly stated that the risk profile assessment is the first and most critical step to be addressed. From a regulatory standpoint, considerable emphasis is put on the appropriateness of the actual risk profile of the fund and the risk profile disclosed to investors.

Pre-investment risk analysis

As private equity and real estate investments are by nature illiquid and designed to be held over a long period of time, selling part of the assets is rarely a possible solution for risk management purposes. In this context, the most critical risk analysis occurs before the investment decision. Such analysis requires in-depth understanding and identification of risks to which the investment may be exposed, such as regulatory, tax, country, political or market risk, and all risks relating to the financing structure, valuation or growth.

Outsourcing will have to be carefully analysed as outsourced activities should not exceed by a substantial margin the functions performed by the AIFM itself

Measuring such risks requires specific skills and knowledge of the industry and of the targeted investee or property, and is only achievable through a comprehensive due diligence exercise. What could or should be the role of the risk managers in the investment process? Should it be challenging or reviewing the due diligence? As a party independent from the pre-investment phase, the risk manager could be of valuable support to the AIFM's governing body in ensuring each step of the due diligence has been thoroughly executed.

Risk measurement techniques: valuation risk, performance risk and beyond

How to measure risks associated with private equity and real estate investments as well as their evolution has been and will remain a very live issue. The lack of quantitative data and the illiquidity of these investments make it very difficult to come up with a short-sighted risk measurement framework such as the Value-at-Risk metric commonly used in the UCITS and liquid financial instruments world. Quantitative risk indicators such as changes in value or volatility of relevant market data (e.g. exchange rates and interest rates), microeconomics (e.g. tenant default rates and rent hikes) and macroeconomic indicators (e.g. GDP growth and inflation rate) can obviously help risk measurement and monitoring, but in light of the very specific nature of those assets, capturing all material risks of private equity and real estate funds and their proper monitoring requires going beyond setting up a handful of periodically updated key risk indicators. Indeed, many risks can materialise in different ways and have a significant impact on a private equity or real estate business (including but not limited to taxes, regulations and competition), meaning that qualitative monitoring and assessment remain the best line of defence. However, such defences require in-depth and close interaction of risk managers with portfolio and asset managers. Some risks may lie within the valuation process itself, such as discount rates and business plan assumptions, and could require close oversight from the risk manager. Risk measurement techniques should enable the risk manager to measure the most material risks at investment and fund level. Going forward, more advanced risk modelling techniques could enable risk managers to combine the various risk indicators in order to derive an assessment and monitoring of performance risk through estimated distributions of internal rates of return over a given time horizon (e.g. IRR@Risk).

Stress tests

Stress testing requirements introduced by the AIFMD are a new (and possibly challenging) factor for many private equity and real estate managers. The results of stress tests are one of the elements that have to be included in periodic reporting to competent authorities, hence the attention paid to them. The implementation of a stress testing framework can be described in four stages: the previously performed risk identification process, definition of scenario, execution of scenario and analysis of results. The definition of scenario could benefit from the involvement of all stakeholders, from portfolio managers to senior management, as a guarantee of appropriateness and integration within the investment decision process. Scenario execution may be performed using a top-down approach, decomposing the fund in relation to a set of exogenous risk factors, or a bottom-up approach, stressing the valuation of each investee or property under a common scenario and deriving the NAV of the fund. The stress testing exercise can, in most cases, leverage from the work already performed in the valuation of private equity or appraisal of real estate properties, by taking a forward-looking view. This work should enable an assessment to be made of the impact of adverse scenarios on the NAV of the fund. Comments on stress test results are also expected to be provided in the periodic regulatory reporting.

Risk monitoring and reporting

The regulatory framework provides no practical guidelines on the frequency or template for the risk management reports required to be submitted to the governing body of the AIFM. Reporting frequency could of course consider frequency of NAV calculation or of Board meetings, and should be at least on an annual basis, but data availability on underlying assets might challenge the ability to provide meaningful reports at a high frequency. The content of the reports should enable senior management to get an understanding of the current risk profile of the fund and of its evolution, including valuation risk, compliance with internal and regulatory risk limits as well as the results of stress tests. It may provide trends and an events update on underlying assets along with any significant risk realisation during the reporting period. Being independent from portfolio management, the reporting provided by the risk manager may enable senior management to take appropriate corrective actions when needed, such as currency or interest rate hedging, or to monitor more closely the evolution of certain risk exposures, such as distance to breaching covenants, political or fiscal risks, exit risks, etc.

Why go beyong regulatory requirements?

This article has tried to illustrate the potential challenges private equity and real estate managers face when implementing AIFMD risk management requirements. In relation to the primary objective, i.e. regulatory compliance, AIFMs can also leverage their risk management function to enhance governance and transparency for senior management, monitor performance risk and meet growing investor demand with regard to risk disclosure.

Improving internal transparency

As described above, we believe a well-structured and independent risk management function will:

- Improve internal risk management skills and capabilities
- Facilitate communication and knowledge transfer between portfolio managers, risk managers and senior management
- Enhance risk oversight, awareness and transparency, including valuation and performance risks
- Help to identify potential shortcomings with regard to future regulatory requirements

Enhanced transparency and communication could also help AIFMs meet the growing concerns of investors on risk-related matters, as well as regulatory reporting requirements.

Meeting investors' expectations

Investors' standards and expectations regarding transparency and disclosure (the 'transparency gap'), as well as general public scrutiny, are likely to increase as real estate and private equity investments become increasingly prominent and visible. That will make sound and effective risk management a genuine marketing argument in a challenging and competitive environment. Delivering value-added risk management reporting to institutional investors could be an opportunity to bridge the transparency gap, helping to shorten the increasingly lengthy fundraising and due diligence processes, and to turn client servicing into asset growth.

How to measure risks associated with private equity and real estate investments as well as their evolution has been and will remain a very live issue

Internal audit
Trends and challenges

Terry Hatherell
Global Internal Audit Leader
Deloitte

Now, more than ever, the internal audit department is recognised as a key pillar in an organisation's overall governance structure. Unfortunate past incidents of corporate wrongdoing and, more recently, risk failures have again served to highlight the critical role that internal audit plays and have shone the spotlight squarely on internal audit to step up and deliver on increasing expectations.

Traditionally, the internal audit function focused on providing core assurance around business process risk and controls. But, with increasing market volatility and complexity, internal audit is being asked to deliver deeper insights and value beyond assurance, particularly in the areas of strategy execution, emerging risk, and increasing the use of analytics. Delivering on these new and increased expectations presents many challenges for internal audit departments today.

An ongoing challenge for internal audit relates to multiple stakeholder expectations which, at times, may differ. It is generally considered that, to ensure the independence of the function, internal audit should report functionally to the Audit Committee of the Board of Directors. Audit Committees, however, have a very clear fiduciary and governance responsibility with respect to value preservation and ensuring that principal business risks are effectively managed across the organisation. These responsibilities translate directly into an expectation that internal audit provide assurance to the Audit Committee (and more broadly to the Board of Directors) that key risks are identified and managed effectively. Without question, this independent assurance role is a basic expectation for all internal audit departments and is at the core of internal audit's mandate. Other stakeholders, including regulatory bodies for regulated entities, have similar expectations of internal audit. Management, as one key stakeholder, looks to internal audit for similar assurances; however, increasingly, management expectations extend beyond this core assurance role in search of greater value—in effect, a greater return for the organisation's internal audit investment. As context for this expanded expectation, one needs to look no further than what is transpiring in many organisations today—a laser focus on creating shareholder value in an uncertain and often challenging business climate.

The expectation of enhanced value is not a new challenge for internal audit departments. What is different today is the confluence of factors—greater complexity which creates new and emerging risks, significant risk failures leading to reputational, regulatory and financial impacts; and an uncertain and challenging economic environment in many regions which has created the need in many organisations to 'do more with less' in order to drive greater shareholder value.

To respond to these challenges and to deliver on multiple and increased stakeholder expectations, highly effective internal audit departments are employing a number of strategies and tactics.

As the business landscape for most organisations becomes increasingly complex and fast-paced, there is a movement towards leveraging business analytic techniques to refine the focus on risk and derive deeper insights into the organisation. Leading internal audit departments are moving beyond the use of ad-hoc analytics that have traditionally provided hindsight and into areas of continuous auditing, sustainable analytics, the application of exploratory and predictive methods and sophisticated data visualisation techniques—all of which deliver profound fact-based insights and foresights. Leveraging analytics allows internal audit departments to produce deeper insights and conclusions that help decision-makers take action quickly and make more effective, timely decisions. At the same time, the use of analytics allows internal audit departments to be more efficient and 'do more with less' by analysing entire populations of data rather than reviewing and assessing samples of transactions. Advanced analytics capabilities also incorporate a predictive element to provide foresight into risk events before they occur. Examples of high-value areas where analytics is being embedded into internal audit activities include predictive project analytics to

assess the effectiveness of project risk management and the likelihood of project success as well as vendor cost recovery reviews to identify duplicate and inappropriate billings and to assess related vendor governance and expenditure controls.

Increasingly, internal audit departments are also including a specific focus on emerging risk. Some internal audit departments have even allocated a defined percentage of internal audit resources to focus exclusively on the evaluation of emerging risk areas. With the explosion of new technologies and the ever-accelerating pace of technological innovation, it comes as no surprise that many of these emerging risks are technology-related. Threats posed by cybercrime, for example, have increased faster than the many organisations' ability to cope with them. Today's cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile and long-term presence within information technology environments. And many organisations risk leaving themselves vulnerable to cybercrime due to a false sense of security, perhaps even complacency, driven by non-agile security tools and processes. Cloud computing is another example of an emerging technology risk and represents a major change in information technology architecture, sourcing, and services delivery by giving businesses on-demand access to elastic and shared computing capabilities. The adoption of cloud computing creates new risks beyond the more obvious security-related risks such as those associated with regulatory, privacy, data integrity, contractual clarity, business continuity and vendor management issues, to name just a few. Other emerging risks include mobile payments, social media, big data and risks related to the extended enterprise created by virtue of the increased use of outsourcing and third parties in businesses today.

With the onslaught of regulations impacting organisations and the expectation that the regulatory environment will become even more stringent, internal audit departments are focusing proportionately more time on assessing compliance with regulations. One such critical area relates to anti-corruption. Beyond the steep regulatory, legal, and financial consequences of non-compliance with anti-corruption legislation, reputational impacts can have severe and long-lasting effects. The Foreign Corrupt Practices Act (FCPA) (which makes it illegal for U.S. citizens or companies to attempt to bribe foreign officials in order to gain a business advantage) and the UK Bribery Act of 2010 are two such examples of regulations with an impact on a global scale. Given the significant risks involved, it is imperative that organisations have anti-corruption programmes in place to ensure compliance. Key elements of an effective anti-corruption program include board oversight, written standards and policies, risk assessments, communications and training, monitoring and auditing, incident reporting, corrective actions, and discipline. Leading internal audit departments are reviewing the design and effective operation of their organisation's anti-corruption programme and are providing independent assurance to management and the audit committee that key anti-corruption risks are managed to an acceptable level.

The recent financial crisis in many regions has highlighted the extent to which a risk and control culture can shape, for better or for worse, the awareness, attitude, and behaviour of employees toward internal and external risk and the management of risk within an organisation. An organisation's culture has a pervasive impact on how its individual members behave. As a result, organisations as well as regulators and government bodies have realised the crucial role that risk and control culture plays in the way risks are managed. In the 'people, process, and technology' trinity of risk management infrastructure, it is indeed people who ultimately make process and technology work. Furthermore, how people manage risks largely depends on the culture prevailing within the organisation. Increasingly, boards and senior management are considering actions to foster a stronger risk and control culture within their organisation. Leading internal audit departments are designing culture assessment frameworks and are executing internal audit activities to assess whether the prevailing risk and control culture and related processes, actions, and 'tone at the top' align with the organisation's values, ethics, risk strategy, appetite, tolerance, and approach.

As the risk landscape becomes more complex and specialised, internal audit departments are challenged to keep up in terms of having the skills necessary to competently assess critical risks impacting their

organisation. Increasingly, leading internal audit departments rely on third-party expertise to provide specialised skills to supplement existing in-house resources. Information technology skills are the most common area where third parties support internal audit departments in bringing much-needed expertise in areas such as security, analytics, information technology governance and enterprise system-specific skills and experience. Additional non-technology specialised skills that internal audit departments frequently seek from third-party partners include regulatory, supply chain, anti-corruption and fraud-related competencies.

Stakeholder recognition of the importance of internal audit has never been greater. As a result, the expectations of internal audit with respect to risk assurance and the provision of insights continue to increase in lock-step. The challenge for the internal audit department, today, is to seize this unprecedented opportunity to cement its value proposition and position itself as a critical element in the overall governance ecosystem.

The recent financial crisis in many regions has highlighted the extent to which a risk and control culture can shape, for better or for worse, the awareness, attitude, and behaviour of employees toward internal and external risk and the management of risk within an organisation

Internal audit in an AIFMD world

Jérôme Sosnowski
Director
Business Risk
Deloitte

Giulio Brenna
Manager
Business Risk
Deloitte

The choice of the internal auditor in this context will prove just as crucial, since it will be difficult, often just for the obvious reasons of cost, to have a permanent, full-time employee within the company

Introduction

The enactment of the Law of 12 July 2013 on Alternative Investment Fund Managers (AIFM) has introduced new challenges for the alternative asset management industry. The demand by regulators, both at European and at Luxembourg level, for enhanced risk governance and risk management accountability at board and executive level, has reached unprecedented levels and is extended from now on to management companies managing non-Undertakings for Collective Investment in Transferable Securities (UCITS) funds, while, at the same time, the law also clarifies and broadens the role and duties of banks through their depositary function for non-UCITS.
In the new regulatory framework, the role and the importance of the internal audit function has taken on a new dimension: as well as becoming a regulatory obligation within all types of AIFM, internal audit now has an advisory role at board and executive level within the organisations impacted by the AIFM law. In addition, new competencies will be required in order to properly cover enhanced technical areas.

Enhanced role of the internal audit function within AIFM

The difference compared with UCITS regulations is significant, as all AIFMs now have to establish a permanent internal audit function. All funds under AIF status will be required to pass from an 'uncontrolled situation' or 'controlled at a minimum' to a situation equivalent to the one of management companies operating under Chapter 15 status. The requirement goes even further in the case of self-managed hedge funds, which unlike their equivalents under UCITS law, must also have a permanent internal audit function.

In such a situation, there are at least two crucial issues for AIFMs to address. First of all, how do you get these companies to focus on the need for a permanent internal audit function, when they often have neither the relevant knowledge nor expertise? The second question is: how do you choose a good internal auditor?

The first key factor will be the awareness of the corporate body ultimately responsible for the sound management of the AIF: the board of directors. The board should be in a position either to directly discuss the results of the work of internal audit, to appoint the internal auditor, to set the roles and the responsibilities of the function in an internal audit charter or to delegate this responsibility to an audit committee. The audit committee will, ideally, comprise three members whose responsibilities will be to cover all internal audit-related matters and the external audit questions, as well as the second line of defence (i.e. the compliance function and the risk management function)—when not delegated to a separate risk and/or compliance committee. In all cases, the roles and responsibilities of the board of directors will be significantly reinforced: to correctly address this situation, it will have to appoint members with internal audit expertise.

The choice of the internal auditor in this context will prove just as crucial, since it will be difficult, often just for the obvious reasons of cost, to have a permanent, full-time employee within the company. Similarly, it will be difficult for self-managed funds, for reasons of independence, to appoint an internal auditor for the fund sponsor or a service provider where operational activities have been delegated.

In light of the above, the outsourcing of the internal audit function appears as one of the solutions to be considered, especially if the individual chosen has already developed a strong expertise in running the internal audit functions of other management companies in Luxembourg. In addition, the firm appointed to the role of internal auditor, if well-chosen, will be able to provide access to a wide range of specialists who will add significant value.

However, it is worth remembering, in this context, that the quality and professionalism of the service provider chosen for the outsourcing of the internal audit function is of paramount importance, and that the board is solely responsible for the quality of internal audit services that will be delivered by the third party. A decision taken only on the basis of cost reasons would be an unwise move, with potentially dramatic consequences for the AIF, AIFM, board members, and lastly, the investors.

New areas of focus for internal audit policy under AIFM

While in many of its aspects, the AIFM law is similar to the UCITS regulations, especially regarding operational matters (e.g. remuneration, conflicts of interest, delegation), new areas of focus are emerging that will have to be included in the internal audit policy. These new areas are:

- **Risk management**
  As with UCITS, each AIFM will have to implement a risk management function and respect its independence from operating units, including matters relating to portfolio management, in accordance with the principle of proportionality. The internal audit function will of course have to monitor, on an annual basis, that the risk management function has been implemented according to these principles, but its role will also be to ensure that the risk management system taken as a whole is appropriate "*to identify, measure, manage and monitor all risks relevant to each AIF investment strategy and to which each AIF is or may be exposed*".
- **Liquidity management**
  For each open-ended AIF that the AIFM manages, it will have to employ an appropriate liquidity management system and implement a management system that will enable it to efficiently monitor the liquidity risk facing each AIF. The role of the internal auditor will be to test the liquidity management system developed by the AIFM and to review its liquidity risk management procedures, the stress tests performed by the AIFM and the coherence between its AIFs, the investment strategies, the liquidity profiles and the redemption policies.
- **Asset valuations**
  This point is probably the most sensitive, mainly because of the nature of the assets in which AIFs invest, e.g. real estate, infrastructure, artworks, land, plantation, etc. The types of assets are so diverse that it is not possible to use a single methodology to obtain the fair value.

  Choosing the correct asset valuation methodology is thus a challenge for asset managers. The method by which assets are valued is determined by a number of variables, such as the underlying asset itself, the reason the asset is held, regulatory guidance and prevailing market conditions. Once the valuation method has been selected, it is important to ensure that adequate controls are in place to value the assets accurately using this methodology. This could mean ensuring the accurate capture of asset cash flows, or alternatively, ensuring that up-to-date and accurate market information is obtained. Furthermore, having appropriate systems and controls in place will help to manage valuation difficulties and guard against questionable prices going unidentified.

  While the role of the internal auditor in this specific case is not to ensure that the valuation of assets is correct (this is the role of the external auditor), the internal auditor will have to ensure that the rules applicable to the valuation of assets are *"laid down in the law of the country where the AIF is established and/or in the AIF management regulations or instruments of incorporation"*. In order to prevent any conflicts of interest, the internal auditor will also have to ensure that the valuation function, whether it is under the responsibility of a third party or within the AIFM organisation itself, is independent, and respect the rules defined in the AIFM Law.

- **Fair value**
  In this environment, determining 'fair value' and what constitutes fair value is becoming increasingly complicated. There is indeed a number of additional factors to consider:
  - Is the input used representative of a price that is observable in an active market?
  - Is trading activity thin and the last price stale or not representative of the fair value on the date of valuation?
  - Is a discount warranted where market participants would not be willing to transact at the quoted price?
  - Is the price accessible to the entity in its principal market?
  - Does the last trade result in an anomalous price relative to other trades on the date of valuation?

  Internal audit can assess the existing valuation process to identify areas where additional procedures should be implemented to ensure that the robustness of the process is consistent with market expectations in determining fair value. This function can also analyse the valuation inputs used and assess whether they are representative of fair value on the valuation date by examining whether all necessary fair value considerations have been incorporated into the valuation process.

- **Broker quotes and pricing services**
  Currently, there is increased pressure on the entity performing the procedures to understand the quotes received from brokers, the pricing services and how the valuations have been determined. In this context, asset management entities may consider the following:
  - Is the broker internationally recognised?
  - Are multiple quotes available, and comparable within an acceptable variance threshold?
  - Is the quote price reflective of a market that the entity can access and transact in?
  - Does the broker trade or make a market in the quoted security?
  - Is the quote based on recent trades or on a valuation model?
  - What are the significant assumptions used in the model?
  - Are inputs based on available/observable market data?
  - Was the model subject to price validation procedures by the broker?
  - Are the inputs the same as those used for the entity's books and records?

While the role of the internal auditor in this specific case is not to ensure that the valuation of assets is correct

To respond to these concerns, the internal audit function may assess the reliability of the price obtained and whether it is reflective of the fair value of the security. It should also understand the inputs and assumptions used by the broker and challenge the reasonableness of the inputs and assumptions used and the appropriateness to the entity. Finally, the internal audit function will have to compare the consistency of inputs and assumptions used with those included in the entity's books and records.

The focus on these particular areas that fall under the scope of the internal audit function evidences that, more than being an expert in internal audit, subject matter experts will have to be involved in order to ensure an appropriate review of the most sensitive techniques. Depending on the complexity of AIFs managed by AIFMs, the impact on the internal audit budget will also have to be adjusted in order to enable the function to cover the most complex activities appropriately.

Enhanced role of depositary banks

Should the new regulatory obligations lead to significant changes in the internal organisation of AIFMs, the depositary function of banks will also have to be controlled carefully by the internal audit function, for the following reasons:

1. The first main impact identified for depositary banks relates to the new regulatory obligations of AIFM Law, which can be summarised into three main key areas:
   - *"The depositary shall be liable to the AIF or to investors of the AIF, for the loss by the depositary (…) of financial instruments"*, meaning that in the event of a loss, the depositary will have to provide compensation or return a similar financial instrument of the same type. The depositary can be considered not liable only if the asset was not a transferable security capable of being safe kept or if the loss was due to an "*external event beyond reasonable control"*
   - The extension of safekeeping responsibility meaning that:
     - Collateral provided to or provided by a third party is considered to be an asset held in custody if the AIF retains or receives title to the collateral
     - The prime broker will have to be considered as the sub-custodian

- The depositary's asset supervision duties apply to funds that are held in a nominee account in the name of the depositary
- For fund of funds, the depositary's asset supervision duties apply on a look-through basis when the underlying fund does not have a depositary or is domiciled in a third country that is not deemed as equivalent for AIFMD

• The new depositary duties:

- Cash management duties where all cash flows associated with the fund, including cash not held with the depositary, will have to be monitored by the depositary
- Subscription/redemption monitoring to ensure that all payments made by or on behalf of investors for the subscription of shares or units of an AIF have been received and booked in one or more cash accounts. The depositary should ensure it receives the relevant information it needs to properly monitor the reception of investors' payments from the AIFM
- The depositary must ensure that appropriate valuation policies and procedures for the assets of the AIF have been implemented
- The depositary has to set up a procedure to verify, on an ex-post basis, the AIF's compliance with the applicable laws and regulations and the AIF rules and instruments of incorporation
- The depositary must ensure that income is probably received and should verify the completeness and accuracy of the income distribution, and more particularly, the dividend payments

2. In addition to these new obligations, the internal auditor will have to pay particular attention to additional elements, such as the client acceptance/ risk profile, the operating model, the monitoring process of the applicable risk model, the escalation and reporting performed by the depositary bank to internal committees/external parties and regulators and contracts

The AIFM Law clarifies and broadens not only the role and duties of AIFM but also the ones of depositary banks' role and duties for all non-UCITS funds, including in light of the UCITS V directive.

Internal audit will have to understand the regulations, know how to pragmatically ensure that in all situations rules will be respected, and proactively advise the management, providing appropriate recommendations to prevent risk crystallisation and add value to the company's governance, risk management and control processes.

The internal audit function will have to compare the consistency of inputs and assumptions used with those included in the entity's books and records

Single Supervisory Mechanism
Trends and challenges

Clifford Smout
Partner
Audit
Deloitte

Simon Brennan
Senior Manager
Audit
Deloitte

Dea Markova
Assistant Manager
Audit
Deloitte

In May 2012, the outlook looked bleak for the Eurozone. In several Eurozone countries, banks and sovereigns were caught in a downward spiral, each undermining the strength of the other, driving indebtedness ever higher. In order to restore confidence in banks and the Euro, policymakers concluded that a multi-pronged strategy was needed. The Banking Union was born, combining a supervisor for Eurozone banks that would be seen as neutral, strong and consistent, a common resolution authority and a fiscal backstop in case resolution funds were exhausted.

Fast-forward to November 2013 and the first pillar of the Banking Union became a reality, with EU Regulations setting up the Single Supervisory Mechanism (SSM) entering into force. The SSM, responsible for the prudential supervision of Eurozone banks, is designed to ensure that all stakeholders can have full confidence in the quality and impartiality of banking supervision, and that there is a credible starting point for the measures necessary to recapitalise banks directly.

The other pillars of the Banking Union are a single rulebook for banks in the single market, a harmonised deposit guarantee scheme, and a single European recovery and resolution framework (the Single Resolution Mechanism—SRM). Progress is being made on all fronts, however, the immediate priority for banks is the SSM.

Drawing on insights from Deloitte member firms across the Eurozone, this article sets out what is happening on the ground, where the SSM is heading, and where firms should focus their attention. The subject is primarily of interest for those banks that will be directly supervised by the ECB for prudential purposes, but all Eurozone banks will be affected by the SSM and should take note. The largest non-Eurozone EU banks should also follow developments carefully: they will be required to conduct an Asset Quality Review (AQR) exercise in 2014 under new EBA guidelines, and will take part in the EBA stress-testing exercise alongside the largest Eurozone banks.

The SSM landscape is becoming increasingly complex. Staying on the front foot by keeping track of developments and coordinating SSM-related work across the organisation will enable banks to manage the challenge strategically. It will also support them in setting the right tone for the new supervisory relationships that are being established with the ECB.

Taking stock

In a nutshell, under the SSM the European Central Bank (ECB) will be given extensive micro- and macro-prudential powers. All of the Eurozone's circa 6000 banks (formally, credit institutions) will fall under the SSM's remit, although the ECB will not directly supervise all of them. Banks have been designated as 'significant' or 'less significant', based on criteria that establish the size and importance of banks to the sectors in which they operate. The ECB will directly supervise banking groups designated as significant, which currently number 124. Supervision of these banks will be conducted by joint supervisory teams, headed by ECB staff and supported by experts from national supervisory authorities. 'Less significant' banks, on the other hand, will remain under national supervision.

The ECB is engaged in two parallel tracks of work during the transition to the SSM—which is scheduled to 'go live' in November 2014. The near-term focus for banks is the ECB's comprehensive assessment. The ECB announced in October that it will subject the 'significant' banks to a three-stage health check: an initial supervisory risk assessment, an Asset Quality Review (AQR) and a stress-testing exercise. This process has started, leading to a surge of data requests from national supervisory authorities.

The second track encompasses the work needed to make the SSM operational. A key element is recruitment, where the ECB is making steady progress. The appointment of Danièle Nouy, Secretary General of the French Prudential Supervision Authority (ACPR), as chair of the SSM in December was a key step forward. Her appointment enables the ECB to make further decisions on appointments to the SSM senior management team, which in turn will facilitate appointments to middle-management and junior positions in supervisory teams. Between 800 and 1,000 individuals will join the SSM by the end of 2014.

In turn, the SSM senior management team can begin to take policy decisions. Ms Nouy has already taken the opportunity to address some of the challenges for the SSM, such as the treatment of sovereign debt and accountability, during her confirmation hearing with the European Parliament Economic & Monetary Affairs Committee in December.

Beyond recruitment and the comprehensive assessment, less is known publicly about the remaining SSM preparatory work streams, which include finalising the design of the supervisory approach. The ECB is expected to consult in Q1 2014 on a Framework Regulation on the way it will cooperate with national supervisory authorities. It is also in the process of finalising the SSM Supervisory Manual—which by one estimate runs to 700 pages, although it is unclear whether and when this document will be made public, or how the Manual will be aligned with the Supervisory Handbook, which the European Banking Authority (EBA) is putting together on a pan-EU level.

Asset Quality Review: known unknowns

Work on the comprehensive assessment is progressing quickly. Banks were asked in October and November to provide data to assist supervisors in the initial stage, the supervisory risk assessment, which involves a quantitative and qualitative analysis of each bank's risk profile.

The first real practical challenge though for banks comes from the next stage, the AQR. The ECB asked banks to provide consolidated balance sheet data at the end of 2013—segmented by asset class and residence of borrower/counterparty—to inform portfolio selection for the exercise. The ECB's intention to be thorough is borne out by the breadth of data that has been requested. However, the data requests to support the next stages of the comprehensive assessment, the AQR proper and the stress test, will be an order of magnitude greater in terms of complexity and volume.

The assessment will cover credit and market exposures, on- and off-balance sheet positions and domestic and non-domestic exposures. The AQR will focus on the riskiest or most opaque components of each bank's balance sheet. Reviews will be conducted by national supervisory authorities, under guidance from the ECB. In most countries, national supervisory authorities plan to engage professional services firms to provide assistance.

The AQR will involve checking the valuation of assets, the integrity of reference data and related controls and processes. The specific objectives of the ECB are to provide an assessment of adequate provisioning for credit exposures, to determine the appropriate value of collateral for credit exposures and to assess the valuation of complex instruments and high-risk assets on banks' balance sheets.

Banks should invest time now and build sufficient capacity to stay ahead, not least as the tasks will become significantly more complex. Key questions remain regarding how the AQR will be organised, in addition to the uncertainty about the data required. For example, the depth of the due diligence phase covering valuations, descriptive data, and controls and processes, is yet to be fully understood.

Beyond recruitment and the comprehensive assessment, less is known publicly about the remaining SSM preparatory work streams, which include finalising the design of the supervisory approach

Looking forward

Although the AQR will occupy minds in the near-term, firms should not lose sight of the stress-testing exercise. The ECB and EBA plan to publish further details in January. And then for some firms, capital shortfall remediation, and remediation of problems identified in controls and processes, will probably come into play in the autumn.

Looking further into the future, lessons can be drawn from the comprehensive assessment, which serves as a pilot for the ECB's supervisory approach in 'business as usual'. In particular, the first stage of the comprehensive assessment, the supervisory risk assessment, will become the modus operandi for risk assessment under the SSM. The way the ECB approaches cooperation with national supervisory authorities, data requests and qualitative and quantitative assessment of risks in its risk assessment will be indicative of the style of supervision firms will experience under the SSM.

We know that as part of that assessment, the ECB will review both risk levels and risk controls across ten categories, including credit, market, operational and liquidity risk, as well as inter-risk concentration and insurance or financial conglomerate risk. The approach is intended to build on existing national practices, as well as leverage off the EBA's Guidelines for the Joint Assessment of the Elements Covered by the Supervisory Review and Evaluation Process (SREP). Data related to assessing risk levels will be gathered quarterly, whereas assessment of risk controls will be annual. The frequency of assessments themselves will depend on the nature of the risks being assessed, with liquidity risk monitored more frequently.

Judgements will have to be harmonised across the supervisory teams. There will be a learning curve for supervisors as they work towards this objective. The ECB's approach to supervision will be data-heavy, which for some banks (and supervisors) may mean more data-centric than the approach they are accustomed to. Another difference will be the ECB's emphasis on peer-group analysis in its supervisory assessment. This approach will create some novel cross-border comparators.

The new supervisory regime: final reflections

Moving responsibility for prudential supervision for the largest Eurozone banks to the ECB will improve the coherence of group supervision, as home and host supervisors for Eurozone entities of a group effectively become one. This in turn will influence the number of supervisors inputting into a group's supervisory college and, for the G-SIBs, Crisis Management Group. It should also allow the home supervisor (the ECB) to have a better overview of risk across the group, as well as how the risks and risk controls of one institution compare to its peers and to the system as a whole.

The creation and management of the new geographically-remote regulatory relationship will introduce new challenges though, with the move to a (partially) twin-peaks model of supervision, where prudential authorities and conduct of business authorities are distinct. There are potential benefits to a twin-peaks approach, but it also introduces novel challenges. For example, the balance between micro-prudential supervision, financial stability and consumer protection can become an issue. The European Supervisory Authorities have always had consumer protection on their agenda, but in the past few years this priority has been pushed back by work on the single rulebook. Possibly, the move to SSM will increase the need for more harmonised conduct of business supervision across the EU.

All in all, the supervisor is an important stakeholder for any bank. The relationship should be addressed with the appropriate level of care and concern. Banks will need to understand the ECB priorities and lines of accountability to know, on the one hand, what makes their new supervisor tick and on the other, what aspects of their bank's business could potentially be a cause of concern. The appropriate channels for internal relationship management will have to be adapted to the new landscape. Here, as elsewhere, it will be important to address such issues proactively.

We know that as part of that assessment, the ECB will review both risk levels and risk controls across ten categories, including credit, market, operational and liquidity risk, as well as inter-risk concentration and insurance or financial conglomerate risk

Strategic balance-sheet management
The quest for performance

Arnaud Duchesne
Senior Manager
Business Risk
Deloitte

The new regulatory landscape

Five years ago, the collapse of investment bank giant Lehman Brothers triggered a series of cascading effects in the financial markets, leading to a crisis that spread outside the banking ecosphere and seriously damaging most western economies and governments. Rule-makers around the globe have worked since then to design new (or strengthened) regulations to prevent (or limit) the occurrence of similar scenarios in the future. In Europe, this has led to a series of Directives and Regulations (EMIR[1], CRD IV[2], SSM[3], etc.) being issued by the European Commission.

This set of new rules has a deep impact on the banks' overall strategy and operating models and should be read together in order to grasp the full extent of their implications. In this article, we will focus of the new Capital Requirements Directive (CRR/CRD IV) that came into force on 1 January 2014.

This new regulatory environment has been designed to mitigate the excesses observed and address weaknesses in prudential regulation, covering the following aspects:

- Increase the quality and level of capital to reduce pro-cyclicality
- Reduce systemic risk and control revenue distribution to shareholders[4]
- Set-up liquidity standards aiming to enhance both the short-term and long-term liquidity profile of financial institutions
- Limit the banks' capacity to leverage their activities

The introduction of the CRD IV is going to introduce additional constraints on financial institutions that will lead to a modification of their balance sheet structures, inducing (all other things being equal) a decrease of the financial institutions' risk profile and, consequently, pressuring those institutions' financial performance.

The objective of this article is to illustrate the potential impacts of CRD IV requirements on the industry as a whole and to present our view on the related challenges for senior management and support functions (CFO, CRO) when managing their company's performance.

1 European Market Infrastructure Regulation
2 Capital Requirements Directive
3 Single Supervisory Mechanism
4 The minimum requirement remains at 8% but the CRD IV introduces capital buffers, but focuses on the quality of own funds through strong emphasis on Core Equity Tier 1

Capital management and its impact on Return On Equity (ROE)

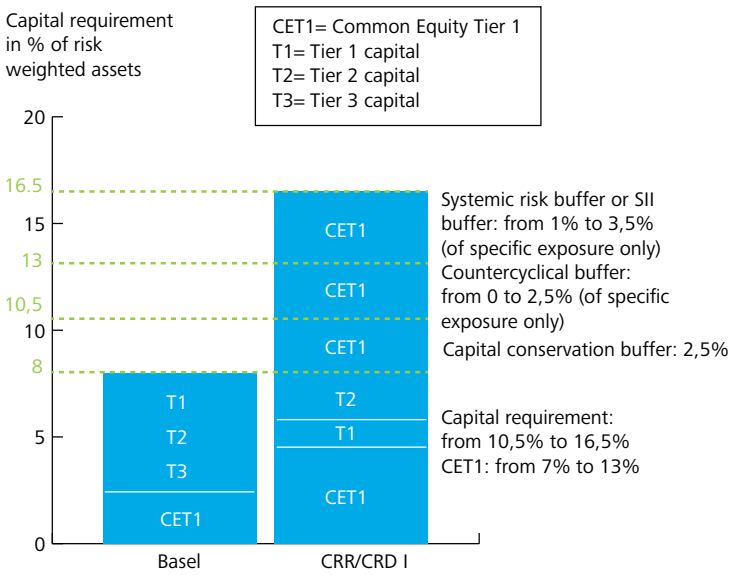
In order to conduct their activities, financial institutions are required to hold a level of own funds that should be large enough to absorb any unexpected losses arising from their activities. In order to estimate the level of own funds that financial institutions should have, banks are required to estimate the level of risks to which they are exposed through their market and credit activities as well as through their operations. To do so, banks either apply a standardised method provided by supervisors or use an internal rating approach also approved by supervisors.

Until now, the solvency ratio of financial institutions, defined as the ratio of the amount of eligible available own funds to the level of risks the bank is exposed to (the so-called Risk Weighted Assets, or RWA[5]), had to be above 8%, with the possibility of having subordinated debt (and similar capital instruments) representing up to 50% of these own funds.

This will gradually change and, when the CRD IV will be fully applicable as of 2019[6], the quality and the level of own funds held by financial institutions will be larger, driven by the following requirements:

- The portion of Tier 1 capital (made up of the most solid capital instruments such as subscribed capital and retained earnings, for instance) in the overall minimum amount of capital shall increase by 50%, from 4% of RWA to 6% of RWA
- On top of the minimum level of own funds (8% of RWA), financial institutions shall hold additional capital buffers, solely made up of tier 1 core equity, with a cumulative buffer size ranging from 2.5% of RWA up to 8.5% of RWA[7]

Figure 1



Rule-makers around the globe have worked since then to design new (or strengthened) regulations to prevent (or limit) the occurrence of similar scenarios in the future

*5 The level of Risk Weighted Assets (RWA) and the level of capital requirements are risk measured expressed on different scales. Capital requirements= 8%*RWA*

6 Between 2014 and 2019, transitional provisions will phase in the CRD IV requirements introduced by the EU regulation No. 575/2013, i.e. the regulation part of the CRD IV (CRR)

7 Depending on the economic cycle and the size of the financial institution

The consequence of these new requirements for financial institutions will be a reduction in the ROE through an increase in equity accompanied by a decrease in the return justified by growth in financing costs together with an increase in taxable revenues.

The increase in financing costs is due to the change in banks' balance sheets as a result of the new regulations. More specifically, financial institutions will have to increase their level of Tier 1 capital for the same business mix. This means that the same amount of assets on the balance sheet will be matched by a smaller amount of debt and a larger amount of equity. As debt is usually a less expensive funding source than equity, this new funding structure should lead to an increase in banks' overall financing costs, despite a probable reduction in the cost of equity.

Why such an increase? According to the Capital Asset Pricing Model, the cost of equity paid by an entity is the sum of the risk free rate and a risk premium multiplied by the beta (ß) of the entity.

cost of equity = risk free rate + ß x risk premium

Depending on the funding structure of the entity, the value of the ß will fluctuate according to the following relationship:

levered ß = unlevered ß x (1 + (1 – tax rate) x D/E))

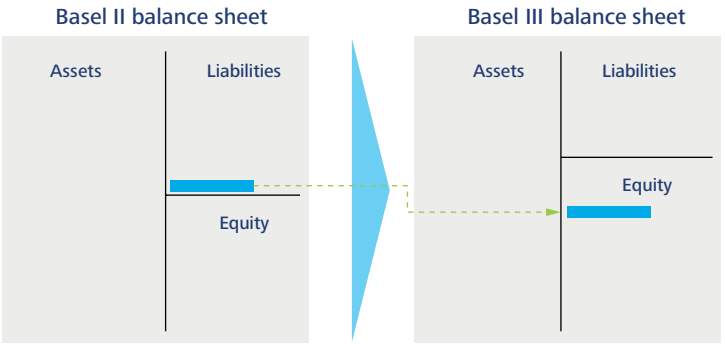
As the debt-to-equity ratio (D/E) will be reduced, the levered ß of banks will be lower, leading to a decrease in the cost of equity.

However, the reduction in the cost of equity should be more than compensated for by the larger share of equity in the bank's capital structure as the portion of core equity more than doubles.

The illustration below summarises the impact of stricter capital requirements on a bank's balance sheet.

Taxable revenues will also increase under the new regulations. As more capital will have to be set aside for a given portfolio of assets, the portion of debt on the balance sheet will be reduced. As a result, interest expenses will be lower, resulting in a higher taxable income.

Figure 2



As debt is usually a less expensive funding source than equity, this new funding structure should lead to an increase in banks' overall financing costs, despite a probable reduction in the cost of equity

Liquidity management and its impact on treasury and ALM

The recent liquidity crisis has illustrated significant flaws in some business models and the weaknesses of several financial innovations. The financial crisis indeed revealed that some banks had become increasingly reliant on wholesale funding and short-term liquidity lines. The weak equilibrium reached in the financial market in 2007 turned out to be extremely vulnerable and ineffective when things went nasty, which translated into the transfer of funding illiquidity to market illiquidity, whereby market participants were forced to sell securities at fire-sale prices, operations highlighting the deterioration of asset prices and bank solvency, creating a vicious circle (procyclicality).

In order to overcome the weaknesses that led to these adverse events, the CRD IV measures introduce a whole new set of regulatory liquidity ratios to measure and improve both the structural health (Net Stable Funding Ratio—NSFR) and short-term liquidity risk profile (Liquidity Coverage Ratio—LCR) of banks, forcing the sector toward a more prudent balance-sheet profile. The impact of these liquidity standards can be quite diverse depending on a financial institution's business mix. Nevertheless, these new standards will lead to a decrease in financial institutions' margins through a reduction in the maturity mismatch combined with a reduction in the return on assets.

With the LCR, the industry will be forced to transfer a part of its core assets into a portfolio made of high-quality liquid assets that will provide lower remuneration compared to its core activities. The impact of the LCR on the bank's performance will depend on the business mix. For example, retail and custodian banks differ widely in their sources of short-term cash inflows (e.g. loans to non-financial customers vs. cash replacement to financial customers) and outflows (e.g. retail vs. corporate deposits) and, as a result, the amount of liquid assets required due to the LCR will also differ.

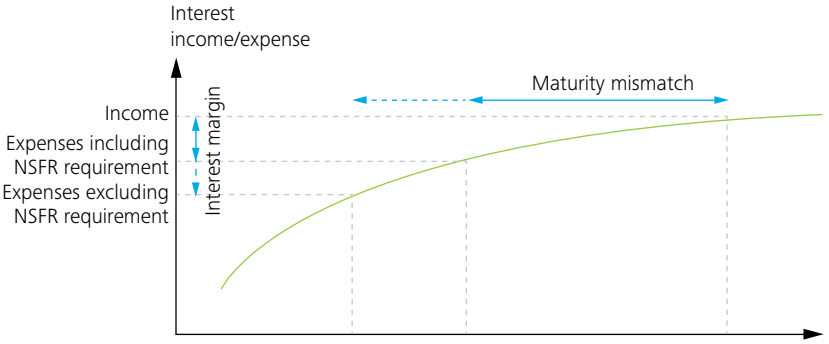
At the same time, the NSFR requires a minimum amount of funding that is expected to be stable over a one-year horizon to cover the liquidity required to finance assets and off-balance sheet exposures. As the NSFR promotes more medium and long-term funding, this will lead to longer-term structural funding of balance sheet items which will reduce the maturity gap between the bank's interest income and expenses. The overall result is a decrease in interest margins, revenues and return on assets.

The figure below highlights the decreasing maturity gap as a result of the NSFR resulting in lower interest margins.

Figure 3

Liquidity coverage ratio (LCR)	= Stock of high quality liquid assets / Net cash outflows over 30 -day horizon	≥ 100%	• Aim to strengthen **short-term** liquidity profile • Defines **level of liquidity buffer** to be held to cover short-term funding gaps under severe liquidity stress • **Cash flow** perspective • Predefined stress scenario • Time horizon: **30 days**
Net Stable Funding Ratio (NSFR)	= Available amount of stable funding / Required amount of stable funding	≥ 100%	• Aim to strengthen **medium to long-term** liquidity profile • Defines minimum acceptable **amount of stable funding** in an extended firm-specific stress scenario • **Balance sheet** perspective • Predefined stress scenario • Time horizon: **1 year**

Figure 4: Interest vs. maturity



The leverage ratio can be seen as a complementary tool to reduce the influence of complex modelling assumptions and calibration procedures on a bank's capital structure

Leverage and its impact on performance

Excessive leverage in (some) banks is widely recognised as one of the factors having contributed to the global financial crisis. Over the past years, financial innovation has fundamentally changed the structure of the financial system. For instance, banks have extensively used credit risk transfer instruments such as structured credit products and have funded a growing amount of long-term assets with short-term liabilities in wholesale markets through the use of off-balance sheet vehicles, exposing themselves to credit and liquidity risk by providing facilities to these vehicles.

In parallel with the structural changes observed in the financial system, risk-based prudential approaches such as the Basel II framework are not designed to fully capture those trends, as non-risky (or risk-mitigated) assets could potentially be piled up definitively in banks' balance sheets such that small deviations from expected risk crystallisation could lead to serious trouble. Inadequate assumptions can lead to a false sense of security and the great dispersion of internal models across the industry emphasises the importance of model risk. A striking illustration of the potential extent of model risk is given by the current regulatory consistency assessment programme conducted by the EU authorities where the preliminary results indicate notable dispersion in the estimated risk parameters assigned to similar exposures[8].

One objective of adding the leverage ratio to the prudential toolkit to complement minimum capital adequacy requirements is therefore to allow an assessment of a bank's capital adequacy that is fully independent of any complex modelling assumptions and calibration procedures. In other words, the leverage ratio can be seen as a complementary tool to reduce the influence of complex modelling assumptions and calibration procedures on a bank's capital structure.

The introduction of the leverage ratio under CRD IV is not accompanied by a specific limit yet. Nevertheless, Basel III advises the setting up of a 3% level, requiring banks to hold a minimum of 3% of Tier 1 capital as a percentage of total assets (and some off-balance sheet items). In other words, any increase in asset value will have to be matched by a corresponding increase in Tier 1 capital (all other things being equal).

To illustrate this, let's consider the mortgage portfolio of a retail bank using the standardised approach to assess its risk. In such a situation, the bank will report a level of Tier 1 capital that will be large enough to strictly comply with the leverage ratio requirement. Under the standardised approach, the mortgage loan portfolio will receive a risk weighting of 35% that will lead to a Tier 1 capital requirement of 35% x 8.5%[9] mortgage loan portfolio exposure. If we estimate the bank has a Tier 1 capital level slightly above the requirement, the leverage ratio will be close to the 3% limit.

8 See "BCBS256 - Regulatory Consistency Assessment Programme (RCAP) - Analysis of risk-weighted assets for credit risk in the banking book"

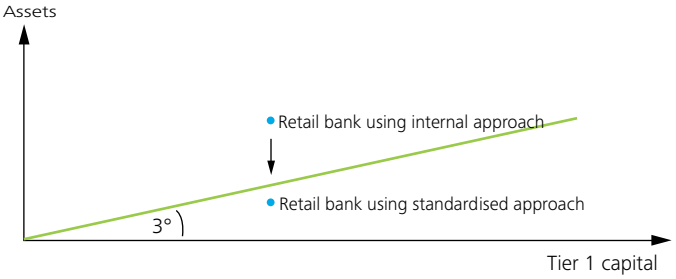
9 CRD IV requires banks to hold a level of 8.5% of Tier 1 capital when considering the impact of the capital conservation buffer, i.e. the counter-cyclical buffer and the systemic buffer are not considered

If the same bank applies an internal model for the assessment of its risk, we can assume that the capital charge for the mortgage portfolio will be lower than the one obtained under the standardised approach. In that case, the bank will be limited by the application of the leverage ratio and will be forced to reduce the size of its mortgage portfolio in order to comply with the requirement. Therefore, it will reduce the performance of the bank impacted by the leverage ratio through an increase of the cost/income ratio[10].

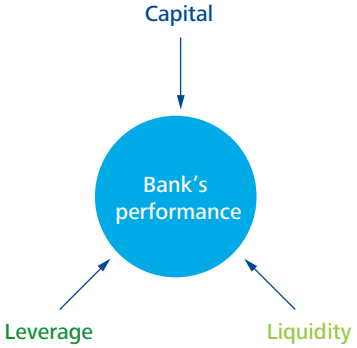
The graph below illustrates the relationship between Tier 1 capital and assets, showing the impact of the leverage ratio, i.e. banks will have to report a level of assets below the green line.

Figure 5

$$\text{Leverage ratio} = \frac{\text{Tier 1 capital}}{\text{Assets}} > 3\%$$



The leverage ratio forces a bank using an internal risk approach to reduce the size of its mortgage portfolio to comply with the 3% level



The industry challenges

The introduction of the CRD IV will change the development of the banking industry, a development that will be driven by funding, capital and innovation in order to maintain the industry performance at an acceptable level. Since the early draft proposals of the CRD IV, financial institutions have started to work on their balance-sheet structures in order to shorten the gaps with the forthcoming regulations. For instance, in July 2013, a large European institution announced a balance sheet reduction of €250 billion over the next two years after having already slashed its size in the first half of 2013. Reducing the balance sheet by almost a fifth will help the bank to lift its leverage ratio to around 3% by 2015. On the other hand, also in July 2013, another large institution announced a series of actions, including an underwritten Rights Issue of £5.8 billion, and measures to improve the bank's leverage ratio.

When the CRD IV will be fully applicable (2019), the industry will have reached a new equilibrium shaped by the new constraints introduced by regulation.

10 In that case, banks will be forced to reduce their asset size, leading to a reduction in income for the same level of cost.

During the transitional phase in which the CDR IV will be progressively incorporated into the economy, banks will have to adjust their business model and their balance-sheet structure in order to maintain their risk/return profile at a level accepted by the financial markets.
The scope of work will be extensive and complex but we believe the industry should primarily focus on the development of an optimal funding structure, a review of their asset allocations, the enhancement of their operations and the setting up of strategic balance-sheet management.

Funding structure

In order to cope with the new liquidity standards, banks will have to find the optimal funding structures that will support their commercial activities at an acceptable cost. Depending on their business model, banks need to respond in a structured way, building a funding structure across instruments, investors and regions.
Given the ambitions of regulators to reduce the importance of the interbank funding channel in order to increase the resilience of the industry in the event of shocks, the industry will have to diversify its funding base through an improvement in their deposit-funding strategies. Amongst others, this development will go through the setting up of innovative funding sources and structures, such as the issuance of new secured-liquid instruments targeting institutional investors, the retail sector, etc.

Asset allocations

With the increase in their cost base, banks will have to increase their Internal Rate of Return (IRR) in order to maintain a profitability level that will be accepted by financial markets and shareholders. This could force banks to tighten their standards for the acceptance of new deals[10], potentially leading to shrinkage of their portfolio that could even force banks out of some businesses. In order to compensate for these losses of market shares, banks will have to review their business model and develop new commercial opportunities in order to ensure proper asset allocations. Nevertheless, the decision to adapt the business model to balance competitive needs will ensure that a bank is taking a decision that is economically viable in the long term.

Enhance operations

In order to offset the probable increase in operating costs (overheads[12] and financial expenses), banks will need to enhance their operations through the development of a solid risk governance framework build upon a central data system and an efficient IT infrastructure. Such an approach will help management access the right information, helping them to improve their reporting capabilities on one hand and overall to monitor business activity on a day-to-day basis. For example, management of collateral at a central level will help the bank to reduce its financing cost through optimal use of those assets.

Strategic balance-sheet optimisation

The increase in regulatory requirements leading to growth in financial costs will force banks' management to address some strategic questions about the maximisation of their returns given their structural balance-sheet constraints. To address these questions, banks will have to improve their resource allocations within these new limits. In order to achieve a portfolio management approach to which banks could apply a Capital Asset Pricing Model, banks need to improve the integration of risks, capital, funding and return aspects. An integrated view of those aspects will help banks to develop a sound transfer-pricing model, helping management with asset allocation exercises and the allocation of resources per commercial segment.

Conclusion

The industry challenges resulting from the introduction of CRD IV will increase the pressure on the bank's management to address these new constraints adequately. The CRD IV will impact not only the accounting and risk functions, but the whole banking organisation from commercial activities to treasury departments. Banks' liquidity and funding management will tend to be an increasingly strategic instrument that will give competitive advantage to institutions that implement proper governance and decision processes.

Together with the ALM functions, the risk management department will need to ensure that emerging trends and regulatory changes are analysed in detail in order to generate appropriate insights for the risk oversight duties of governing bodies (senior management and board of directors) when setting business strategies. To do so, those departments might need to improve the integration and/or the sophistication of their processes (fund transfer pricing, automation of reports, development of central data management, etc.) in order to better capture the various drivers impacting the bank's performance, as well as their interconnection.

Understanding and actively monitoring the various indicators that will track these drivers will no longer be an option when entering this new risk and capital management era.

11 To achieve their new level of return, bank should transfer their costs to clients. All other things being equal, it should lead to a decrease in their volume of activity.
12 Cost of implementation various pieces of regulation (and the associated reporting burden) are expected to be significant in the coming years

Basel III
Principles for effective risk data aggregation and risk reporting

Jean-Pierre Maissin
Partner
Strategy & Operation/Technology
Deloitte

Ronan Vander Elst
Director
Strategy & Operation/Technology
Deloitte

Loic Saint Ghislain
Manager
Strategy & Operation/Technology
Deloitte

What is at stake?

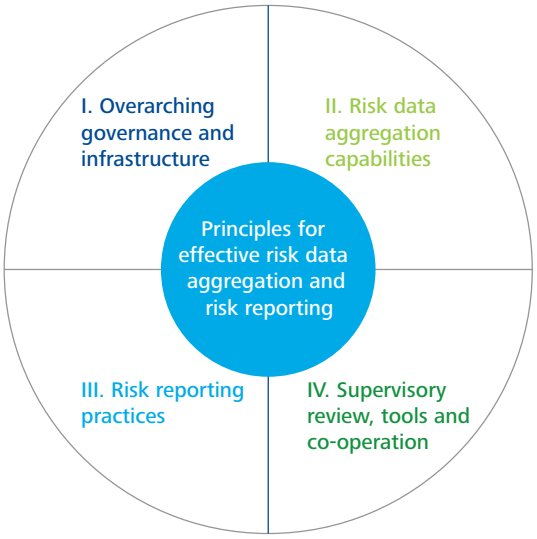
In January 2013, the Basel Committee on Banking Supervision published the BCBS 239 paper: 'Principles for effective risk data aggregation and risk reporting'. The impact of this is significant for Global Systemically Important Banks (G-SIBs), as it defines strong requirements in terms of data management. The objective of this regulation is to ensure that data used for risk calculation and reporting have the appropriate level of quality and that the published risk figures can be trusted. This implies that not complying with these principles would jeopardise the trust of regulators, which could lead to capital add-ons. At this stage, only G-SIBs are concerned, but it is strongly recommended that regulators apply the same rules for local systemically important banks, which may lead to wider scope of application. The timeline for expected implementation is the beginning of 2016.

This new constraint is also an opportunity for banks to improve their operational excellence and increase revenues. Indeed, data quality issues have already been the cause of significant losses through a lack of productivity or incorrect decision making. A significant example of the impact of poor data quality is an online banking provider that lost many customers who opted out of receiving promotional messages from their provider because they had repeatedly received offers for products they already owned.

What are the main requirements?

The requirements are principle-based, and are organised into four categories, the fourth being for the local regulators.

Figure 1: Principles for effective risk data aggregation and risk reporting categories



I. Overarching governance and infrastructure

These principles mainly cover two fundamental aspects of data management: sponsorship and IT infrastructure. The point here is to ensure ownership of the risk data aggregation processes by senior management in order to put in place an appropriate level of controls. This also requires the IT infrastructure to be robust and resilient enough to support risk reporting practices at a time of stress and crisis. For example, risk reporting should be integrated into a bank's business continuity plan, and banks should establish integrated data taxonomies and architecture across their groups.

II. Risk data aggregation capabilities

These principles mainly aim at putting in place the processes and controls prior to risk calculation, notably data quality monitoring, the procedures applied and the documentation produced (e.g. definition of the single point of truth for all data or maintenance of a cross-functional data dictionary). It considers most aspects of data quality, from accuracy to timeliness. It also recommends adaptability of the processes to enable fast decision making.

III. Risk reporting practices

With these principles, data quality is again emphasised in this category, with reference to the accuracy of the reporting made. It also recommends clarity in this reporting, to make it useful for senior management in decision making. For example, it is required to define requirements and processes to reconcile reports to risk data or that the frequency of reports should be increased during times of stress/crisis: *"Some position/exposure information may be needed immediately (intraday) to allow for timely and effective reactions"*.

IV. Supervisory review, tools and cooperation

Finally, this last category relates to the controls regulators will be expected to implement with regard to the above-mentioned principles. Regulators will also be expected to introduce measures that may even involve the use of capital add-ons. For example, supervisors should test a bank's capabilities to aggregate data and produce reports in both stress/crisis and steady-state environments, including sudden sharp increases in business volumes. Supervisors should also be able to set limits on banks' risks or the growth in their activities where deficiencies in risk data aggregation and reporting are assessed as causing significant weaknesses in risk management capabilities.

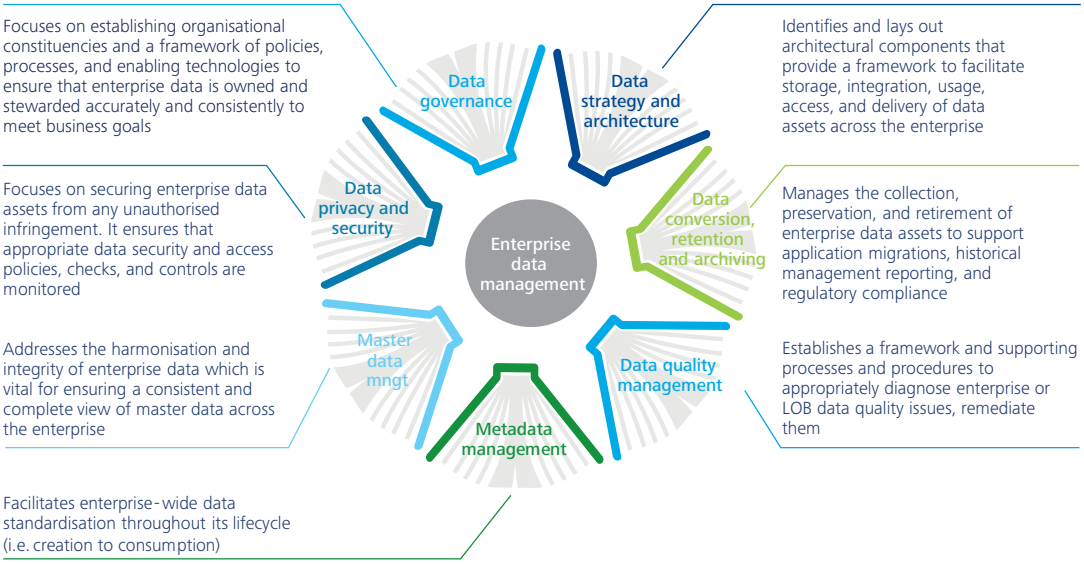
Where is the market today?

Most G-SIBs are aware of the impact of this regulation and are currently formulating plans to meet the regulatory deadline, which is scheduled for the beginning of 2016. The first internal assessments performed showed no major gaps, except in the area of data quality and monitoring (mainly the principles relating to category II above), where some banks will have to make an effort to reach a more mature level. Most organisations have already started internal initiatives (regulatory reviews) that at least partially cover the necessary requirements. The programme to achieve full compliance will be multi-year and compliance with specific requirements is likely to be phased in. Some banks are indicating that full compliance will extend beyond 2015, particularly where significant investment in technology is required. Subsidiaries of the major players headquartered in Luxembourg will also be impacted by this regulation in terms of the reporting they provide to their group.

How can a data management framework help in leveraging opportunities?

Meeting these requirements and seizing the related opportunities require banks to adopt a comprehensive approach to their data. This approach must address the seven aspects of data management (Figure 2):

Figure 2: Enterprise data management framework



The four key aspects are:

1. Data governance

   Data governance consists of defining roles and responsibilities in respect of data and their use. More specifically, it defines who is responsible for ensuring that a data set complies with the organisation's data quality, documentation, architecture, security and retention standards. A key role in the governance structure is the sponsoring executive (Chief Data Officer or Chief Analytics Officer), who will manage the buy-in of people, oversee the cultural shift in the organisation and enable the success of data management projects. We have all heard the story of a risk model *"operated through a series of Excel spreadsheets, which had to be completed manually, by a process of copying and pasting data from one spreadsheet to another"*. This is why proper governance of processes and controls has to be set up.

2. Master data management

   One of the main challenges of master data management is the synchronisation of the referential data throughout the organisation. This implies appropriate processes and architecture to enable reconciliation of data from various sources, as well as their diffusion in the bank.

3. Data quality

   Data quality enables organisations to make initial assessments of their data, and to improve and monitor the quality of their data on an ongoing basis. In this area, it is crucial to centrally define common quality dimensions and standards to ensure uniform data quality and trust across the data users community. It is also essential to automate the quality assessment process to allow business users to focus on remediation actions rather than performing controls.

4. Metadata management

   Risk models, which are sometimes complex, require effective data input. Inefficient data input may lead to the wrong interpretation of results. This can be managed using the data glossary throughout the organisation to have clear and common view on available data and its definition. When embedded in data reporting, metadata management will enable end data consumers to be sure they have the appropriate inputs.

Conclusion

Complying with Basel III requirements, and especially BCBS 239, will be a major challenge for G-SIBs, as this requires a high maturity level in terms of data management. Investments to be performed in this domain represents a significant opportunity to leverage requirements and implement a data-oriented organisation to enhance decision making and client service.

IT implications for Basel III & CRD IV

Jean-Pierre Maissin
Partner
Strategy & Operation/
Technology
Deloitte

Marco Lichtfous
Partner
Capital markets/
Financial risk
Deloitte

Jean-Philippe Peters
Director
Business risk
Deloitte

Mario Deserranno
Manager
Strategy & Operation/
Technology
Deloitte

Following the banking crisis of 2007-2009, the Basel Committee for Banking Supervision (BCBS) initiated a review of its regulatory capital requirements (Basel II framework). Following a series of 'quick patches' to amend some of the existing rules, the review culminated in the release of a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen regulation, supervision and risk management within the banking sector (Basel III framework).

In Europe, this effort has been transposed into three Directives: Capital Requirements Directives II and III for the patches and Capital Requirements Directive IV (CRD IV) for the Basel III rules. The Capital Requirements Regulation (CRR) is the legal act implementing the new Capital Requirements Directive IV.

The CRD IV package will become applicable as of 1 January 2014, even if EU member states have yet to transpose the directive into national law. CRD IV/CRR will require banks to perform a major update to their IT risk landscape, by reinforcing existing principles regarding capital adequacy as well as by introducing new requirements concerning liquidity risk, leverage ratio and risk management in a crisis context.
These changes may result in strategy overhaul, process review and IT system impact.

CRD IV/CRR implications for IT architectures

Financial institutions will face higher regulatory compliance costs with the introduction of the CRD IV/CRR rules issued by the regulatory bodies. CRD IV/CRR will impact the entire financial institution, with implications for business processes, data and technology management.

Processes

Current banking processes will need to be modified to be able to handle the new rules and standards. One of the biggest impacts will be the monitoring of intra-day liquidity and the generation of the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR). Although CRD IV/CRR, will for many banks, just be an extension to the structure put in place for Basel II, the impact on the bank's strategy and processes should not be underestimated. The implementation of the rules and standards will give management a better insight into their business, leading to new opportunities and adapted business processes.

Data

Most of the regulations under CRD IV/CRR have direct implications for the way the bank handles its data. Under the new rules, banks will need to demonstrate data quality and traceability. Ad hoc regulatory reporting requests will mean that the quality of the underlying data will become highly important for the bank. For instance, prudential regulatory reporting will require much more detailed information to be reported to supervisors, to the extent that inconsistencies between reporting documents could affect the bank's reputation and credibility (and lead to sanctions and fines). Banks will also need to source data from different functional areas and cross products. This means that banks must have the necessary processes in place to ensure data integrity. For this reason, the BCBS rolled out new principles for effective risk data aggregation and risk reporting which must be met before 2016 and that will impact the data collection and data traceability processes of the legacy Basel II chain.

Technology

One of the biggest impacts from a technological standpoint is the ability to produce integrated reports, with consistent reporting across the company. Solutions should be able to produce the reports required internally and externally (disclosure reports and regulatory reports). In addition, within the context of the Single Supervisory Mechanism (SSM), there are potentially multiple reporting documents to be submitted to both national supervisors and the local central banks.

IT systems should be flexible enough to cope with the impact of the new regulations and modifications to the bank's changing business strategies. The technology put in place for the generation of the reports should have extensive reconciliation capabilities as the new standards and ratios require close coordination between risk and finance data as they are highly dependent one on another. Solutions will also need to be able to handle the greater detail of real time data to meet the intraday monitoring requirements for the LCR ratio.

Integrated reporting also means that the different in-house and third-party risk calculation applications should be integrated into a single architecture.

Flexible architecture

CRD IV/CRR is one of the steps towards improving the banking sector's ability to absorb shocks arising from financial and economic stress. However, further steps involving reviews of securitisation, trading books and operational risk can be expected. New recovery and resolution plans providing national authorities with common powers and instruments are currently being developed and implemented. This continuous evolution of rules and standards is creating uncertainty about future processes within the banking industry, increasing short-run economic costs. The changes seen in the banking market as a result of CRD IV/CRR are believed by many to be just the tip of the iceberg. With each new implementation of new regulatory accords, banks will face a degree of change in their market and business models. Financial institutions will need to rely on flexible IT architecture to cope with new regulatory accords and the resulting business changes.

Technical opportunities

Financial institutions need not resign themselves to a future of low profitability due to the implementation costs of regulatory rules and standards. Appropriate data management could help banks to become Basel III compliant and more profitable at the same time. Financial institutions can use the implementation of Basel III as an opportunity to streamline their business by using the data architecture put in place for day-to-day management decision-making.

Basel III does not involve a real risk and compliance revolution. However, being able to perform frequent, timely and comprehensive calculations with fresh and accurate data at the right level of detail will be a challenge. The biggest challenge for most banks will not be devising and implementing the more sophisticated risk methods, but being able to deliver ratios based on accurate data.

Today, many banks have to define strategies to manage their risk, finance and compliance functions. These functions are currently often managed as separate silos where each function has its own set of applications. An architecture based on silos makes it difficult to generate a holistic view upon the bank's data. Consolidating the risk, finance and compliance functions will speed up the process of becoming compliant and at the same time drive real competitive advantage. An architecture based on centrally managed data will offer complete visibility and control of risk data independent of its source. It will offer traceable, consistent, high quality data which can be shared across departments within the bank.

Banking data have become the key to successful risk, finance and compliance management. The banks with access to accurate and complete data will be those able to competitively differentiate themselves. To fully benefit from these centralised data architectures, banks must implement a scalable solution that evolves with the business and accommodates existing applications.

How to get there

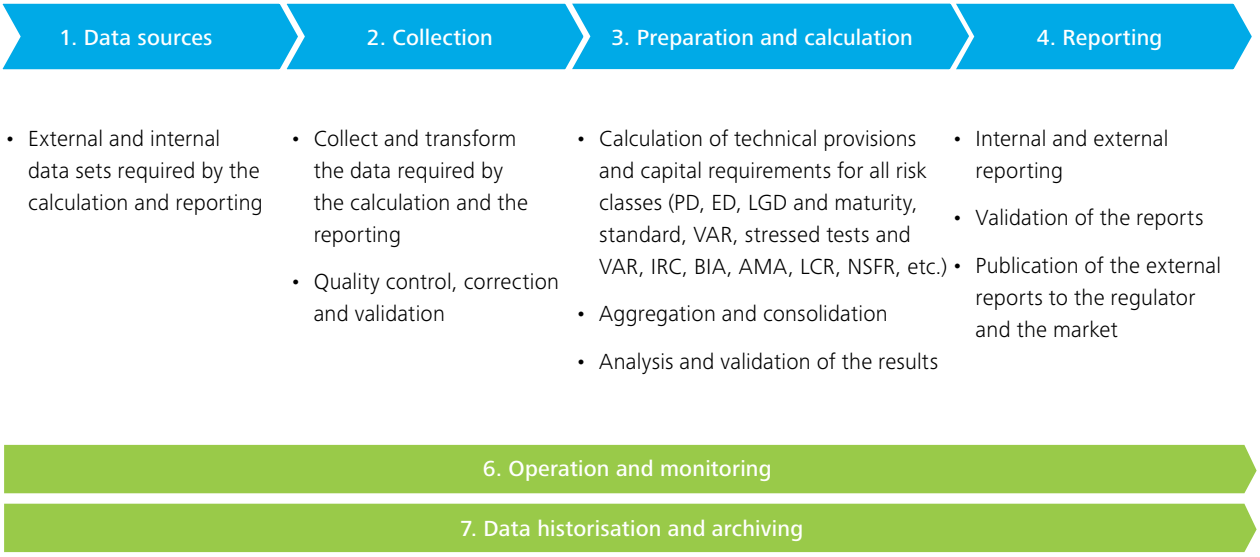
Banks must define a target IT architecture by identifying the areas where components must be added or modified to achieve compliance with Basel III rules and standards. Banks will list the necessary actions to reach compliance via a gap analysis between the current situation and the Basel requirements,

In a second phase, the architecture approach will need to be defined. The most suitable approach will depend on the bank's long-term IT strategy, the stability and performance of the current system, the compliance target date and available resources.

With the IT approach and gap analysis, a make-or-buy decision will determine how the bank will fill the gaps towards compliance. A selection process may determine if a software package provides the right solution.

Integrated reporting also means that the different in-house and third-party risk calculation applications should be integrated into a single architecture

Figure 1



The European regulatory agenda on payments is driving major industry change

Stephen Ley
Partner
Technology Risk
Deloitte

Steve Bailey
Director
Technology Risk
Deloitte

Aurelie Haynes
Senior Manager
Technology Risk
Deloitte

Debs Banerjee
Manager
Technology Risk
Deloitte

On 24 July, the European Commission published long-awaited proposals on the payments market in Europe, consisting of three elements: a revised Payment Services Directive (PSD), a regulation on Multilateral Interchange Fees (MIF) and a communication on SEPA governance.

These sit alongside other regulations including transparency of information for Anti-Money Laundering (AML) and sanctions, the proposal for a directive on the transparency and comparability of payment account fees, payment account switching and access to basic payment accounts. This broad regulatory agenda continues to provide compliance challenges for the financial services sector and impact increasingly on corporates and consumers.

Revision of the Payment Services Directive (PSD2)

The original Payment Services Directive (2007) established a legal and regulatory framework for Payment Service Providers (PSPs) and opened up the market to some non-bank PSPs. The revised PSD2 has been extended to include Third Party Payment Providers (TPPs) in its scope. This will increase competition in the payments market, creating opportunities for innovation, particularly for the offering of services focused on efficiency and reduced cost and making use of technological advances.

Some of the key changes that are proposed in PSD2 are:

Extensions in scope

The Commission proposes to extend the scope of the PSD to require compliance with transparency requirements and the provision of information where 'one leg out' transactions occur, namely transactions where money is being sent out of or into Europe.

Additionally, as a consequence of the dramatic increase in mobile banking and unregulated payment solutions, third-party providers of payment initiation services (which typically operate between the merchant and the purchaser's bank) and account information platforms will be required to be authorised under PSD2 as payment institutions.

Prohibition on surcharges

Currently, under the PSD, different regimes are in place across the European member states in relation to surcharging. Some member states allow surcharges on certain payment methods to enable the funnelling of the payer by the PSP towards the use of the most efficient payment systems. PSD2 will harmonise the surcharge practice by applying a prohibition on surcharging to consumer credit and debit cards under the four-party model. A small proportion of card transactions will not be subject to the regulation (e.g. corporate cards), and surcharging will still be possible by the payee for these transactions, as long as they do not exceed the cost borne by the payee in accepting the payment method chosen by the payer.

Third-party access to payment systems

The PSD has also been extended to cover all e-transactions made through IT devices, e.g. mobile, internet, etc. TPPs will now be able to initiate payments on behalf of consumers. In reality this is a major change to payment industry operating models, as it requires banks to allow TPPs access to their payment infrastructures where the consumer has provided consent and the TPP adheres to necessary security requirements.

Transparency

Under PSD2, transparency and information requirement provisions will increase in scope to also apply to payments made to third parties where only one of the PSPs is located within the EU.

Security

New rules for improving payment security over the internet are also included under PSD2. This requires PSPs and TPPs to ensure that they support two-factor authentication for card-not-present transactions and will adhere to the more detailed security requirements to be published by the European Banking Authority (EBA). An assessment of the operational and security risks at stake and the measures taken will need to be done on a yearly basis.

Single Euro Payments Area (SEPA)

The harmonisation of the euro payments market has been in the offing for a long time and will result in many benefits and efficiencies for companies with material euro flows. To achieve this, SEPA provides a single set of euro payment instruments—credit transfers, direct debits and card payments.

The deadline for SEPA is February 2014 for eurozone countries and October 2016 for non-euro countries. All euro payments will be made via a common payments framework (ISO 20022 XML) using standard bank account details including International Bank Account Number (IBAN), rather than the existing different domestic arrangements in each country. In effect, this will remove the distinction between domestic and cross-border euro payments within SEPA and will replace the country's incumbent local credit transfer and direct debit processes.

Many companies are still a long way from completing their convergence processes. The latest migration report from the European Central Bank (October 2013) shows a near-60% migration rate for the SEPA credit transfer system, but only 7% for the SEPA direct debit scheme, indicating that most companies will be completing their initiatives in extremely close proximity to the February 2014 deadline.

Regulation on interchange fees

The European Commission's first draft of its proposal on Multilateral Interchange Fees (MIFs) (fees paid by banks to each other for each card payment) outlines changes that the Commission suggests will remove important barriers between national payment markets, reduce fees and prevent surcharges being applied to customers, thereby encouraging the emergence of new players.

"A level playing field will be created for payment services providers, new players will be able to enter the market and offer innovative services, retailers will make big savings by paying lower fees to their banks, and consumers will benefit through lower retail prices."
Joaquín Almunia, Vice President, European Commission

The proposal suggests a prohibition on surcharging and imposes a cap on interchange fees of 0.2% for debit cards and 0.3% for credit cards (except for three-party schemes such as AMEX and commercial cards). The cap will initially apply to cross-border payment transactions from when the interchange fee regulation is implemented and 22 months later to domestic transactions. A further aim of the changes is to give merchants the freedom of choice to steer consumers away from more expensive cards.

The Commission expects the result to be cost savings for merchants and, due to the prohibition on surcharging, cheaper goods and services for consumers. The proposals will require significant changes to be made to existing payment service providers' business terms and procedures. Banks may want to look at other potential revenue streams in lieu of interchange fees.

Directive to prevent the use of the financial system for money laundering or terrorism financing

This 2006 regulation regarding information on the payer accompanying transfers of funds was updated in 2013. It increases the scope, and therefore, the effectiveness of legislation combating money laundering and terrorism financing.

The legislation requires companies to maintain records as to the identity of ultimate beneficial owners and provides increased clarity and transparency on customer due diligence rules. It also extends the definition of Politically Exposed Persons (PEPs) to include domestic PEPs.

The scope of the legislation has also been broadened to include gambling and specific provisions on tax and extends to all persons dealing in goods or services for cash payments of €7,500 or more (the previous threshold was €15,000).

Conclusion

Changes in payments regulations will produce both winners and losers, as institutions adapt their current compliance offerings with differing levels of success. The various financial consequences of non-compliance, coupled with high levels of scrutiny by both the media and regulators, mean the penalties for failing to adapt to the changes may be considerable. Further regulation is coming, and it is important for businesses to be adept and agile in their response to the payments compliance challenge.

Challenges	Recommendations
• The level of change from PSD2 (and the previous PSD) impacts the products, operations and customer areas of organisations, and will need support from risk and compliance departments • Assessing the impact of IT changes that will be required by PSD2 to ensure the new requirements are adhered to, such as third-party access to payment systems • Ensuring systems are compliant with new security requirements under PSD2 • Changes for PSD2 and SEPA are likely to require large scale customer communications and amendments to terms and conditions • Regulations can be difficult to interpret and implement, often requiring complex or near real-time reporting structures • Completion of SEPA migration for the February 2014 and October 2016 deadlines and assessment/ leveraging benefits from the regulation, as opposed to just attaining compliance • Caps on interchange fees will challenge business models for issuers and acquirers • New requirements for screening customers must be analysed and their impact assessed	• Ensure an early gap analysis is performed against all product sets to determine the impact and prioritise change activity, providing sufficient time for any IT changes required • Ensure relevant departments such as risk, legal and compliance are engaged early in the process • Review existing security mechanisms and supporting processes against the security standards to be published by the EBA and ensure full adherence to the requirements for two-factor authentication for card-not-present transactions • Review and update relevant control frameworks to embed new controls that will address regulatory requirements • Supporting MI will need to be defined and developed to allow compliance to be evidenced to regulators • A centralised governance process is important to ensure consistency of response across all business areas that are affected • Complete SEPA migration, including conversion to IBAN and IBAN-only payment requests • Assess benefits that can be derived from SEPA, such as cost savings through standardised operating models, organisation, centralised and shared IT capabilities within Europe • Issuers and acquirers will need to review business models including potentially increased card fees and market segmentation given proposed caps on interchange fees • Ensure compliance with new screening requirements and understand the impact in terms of resource requirements to perform and manage additional screening and consider automation to reduce false positives

Cyber security
Time for a new paradigm

Stéphane Hurtaud
Partner
Information & Technology Risk
Deloitte

More than ever, cyberspace is a land of opportunity but also a dangerous world.

As public and private sector organisations continue to move into cyberspace, so do criminals. Cyber-crime, which is the collective term for criminal activities carried out by means of a computer or the Internet, has become increasingly sophisticated, making it difficult to detect and combat. Nowadays, cyber-crime cases appear in newspaper headlines on a regular basis, showing the extent and the ever-evolving nature of the cyber criminality landscape:

- *'US accuses China of new cyber attacks'* (The Guardian, 31 January 2013)
- *'NSA Prism program taps in to user data of Apple, Google and others'* (The Guardian, 7 June 2013)
- *'5 hackers charged in largest data-breach scheme'* (Bloomberg, 26 July 2013)
- *'LulzSec hackers sentenced for sophisticated global cyber-attacks'* (The Independent, 16 May 2013)

According to Deloitte's 2012 Global Financial Services Industry Security Study[1], about one-quarter of all banks were victims of a cyber breach in 2011. The cost of cyber-crime to the global economy to date may already be substantial. Some studies cite figures as high as US$388 billion[2] or US$1 trillion[3] , which is larger than the global black market in marijuana, cocaine and heroin combined (US$288 billion).

In this context, it goes without saying that cyber security is increasingly becoming a key concern among organisational leadership, including boards of directors. A biennial study of enterprise security governance practices by the Carnegie Mellon University CyLab found a sharp rise in board-level attention paid to the topic. Among companies surveyed in 2012, 48% have a board-level risk committee responsible for privacy and security, up from just 8% in 2008.

The cyber security threats landscape

The 2013 Data Breach Investigations Report (DBIR)[4] consolidates information of the data breach incidents in 2012 from diverse sources to facilitate analysing threats a particular industry is exposed to (a total of 47,000 security incidents with a focus on 621 incidents with confirmed data loss). Deloitte is one of the 19 contributing organisations to this report in light of its incident response and investigation services.

Which industries are at risk?

A definite relationship exists between a particular industry and attack motive, which is most likely a result of the data targeted (e.g. stealing payment cards from retailers and intellectual property from manufacturers):

- 37% of breaches affected financial organisations, mainly due to a large number of ATM skimming incidents
- 24% of breaches occurred in retail environments and restaurants
- 20% of network intrusions involved manufacturing, transportation and utilities

What are threat actors and what are their motivations?

There are four main categories of malicious actors in cyber security:

- State actor: the rise of state actors is significant and considered a great threat according to Deloitte. There are several countries that have openly participated in information warfare for the past several years targeting both private companies and governments

More than ever, cyberspace is a land of opportunity but also a dangerous world

1 http://www.deloitte.com
2 Norton Cybercrime Report 2011
3 The Global Industry Analysts; McAfee, 'Unsecured Economies: Protecting vital information' 2011
4 Verizon 2013 Data Breach Investigation Report

- Organised crime: as explained earlier in this article, cyber crime has surpassed the global drug trade in terms of revenue. This is not simply limited to credit card data, but anything of value
- Hacktivist/activist: the hacktivist movement is the newest addition to the threats list. Groups like Anonymous, Lords of Dharma, Team Poison and others have garnered a lot of media attention
- Insider: insiders can range from the negligent employee who loses a laptop to a completely malicious actor who releases confidential data in an act of vengeance

Most confirmed cases of data loss are perpetrated by outsiders, generally by organised crime groups or state-affiliated groups. The largest number of actors reportedly come from China, Romania, the United States, Bulgaria and Russia.

How do breaches occur (threat actions)?
Threat actions describe what the actor did to cause or to contribute to the breach, taking into consideration that every incident contains one or more actions.

- 52% used some form of hacking, including all attempts to intentionally access or harm information assets without (or in excess of) authorisation by circumventing or thwarting logical security mechanisms
- 76% of network intrusions exploited weak or stolen credentials
- 40% incorporated malware—malware is any malicious software, script or code added to an asset that alters its state or function without permission
- 35% involved physical attacks. Physical threats encompass deliberate actions that involve proximity, possession or force (ATM skimming operations, point-of-sale device tampering, stolen user devices, etc.)
- 29% adopted tactics such as phishing, bribery, extortion, etc.

What is the breach timeline?
Understanding the timeline of an incident can greatly increase the ability to assess and improve an organisation's lines of defence.

- In 84% of network intrusion cases, initial compromise (the time taken for the attacker to get his foot in the door) occurred within hours or less
- In 69% of network intrusion cases, initial compromise to data exfiltration (point when non-public information is first removed from the victim's environment) also occurred within hours or less
- In 66% of network intrusion cases, initial compromise to discovery (i.e. when the victim first learns of the incident) took months or more. In addition, approximately 70% of breaches were discovered by external parties who notified the victim

While these statistics highlight the need to improve prevention measures (ability of organisations to resist cyber-attacks), we must accept the fact that no barrier is impenetrable, and detection/response represents an extremely critical line of defence.

Cyber security risks are not new, so what is different?

The digital revolution is driving business innovation and growth, but also exposing organisations to new and emerging cyber threats. The threat landscape has changed, and the business case for more mature cyber security is better than before. Actually, new business goals and new ways of working are driving business innovation and growth, but these expose us to new and emerging cyber security threats:

- **Consumerisation** ('bring your own'): de-perimeterisation and loss of control of data and devices that have left the traditional data centre boundaries
- **Increased collaboration:** cross-channel, cross-platform sharing of large volumes of sensitive data
- **Technology innovation:** lack of understanding of risks introduced by new tools and processes
- **Commoditisation of IT** (e.g. cloud computing): business functions can procure IT services outside of internal controls
- **Market trust:** reputational damage of a cyber-attack destroys trust which is very hard to recover
- **Globalisation:** new threats arising from expansion into new markets and new ways of working

As organisations increasingly adopt cloud, mobile and social computing, IT environments are becoming more difficult to defend.

Technology

Cloud
Social
Virtualisation
Mobile
Analytics
Shared services

Threats

Nation states
Criminal syndicates
Patch failure
Espionage
Hactivists
Insiders

Most confirmed cases of data loss are perpetrated by outsiders, generally by organised crime groups or state-affiliated groups

The need for a cyber resilient organisation

As illustrated earlier in this article, the adoption of new technologies and the emergence of new threats result in a more complex risk landscape. In this context, many organisations may not be as effective at managing cyber threat risk as they are at managing risk in other areas.

Cyber resilience requires that organisations have the agility to prevent, detect and respond quickly and effectively, not just to incidents, but also to the consequences of the incidents.

First of all, it's essential to understand the cyber threats to your organisation before you can develop an effective cyber security strategy. For example, cyber risks can be mapped according to three factors:

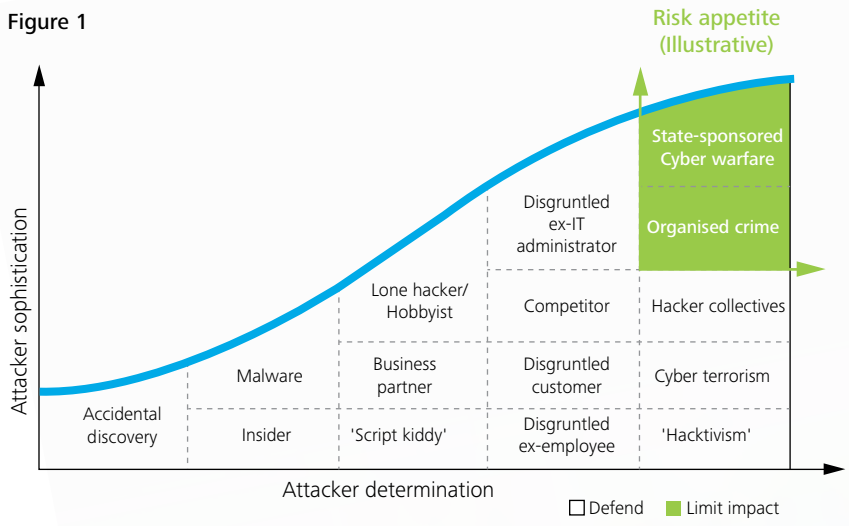
- Does the organisation focus on preventing the risk or detecting and responding to it if it occurs?
- Is the risk known and understood (does it relate to a current threat?), or unknown with little or no understanding (a future threat)?
- What level of concern does the risk pose?

The maturity of an attacker can be measured by their sophistication and determination. Those that are more mature are harder to stop, and there is a decreasing ROI on controls that prevent the most mature attackers. Depending on your risk appetite and the threat landscape for your organisation, one option may be to focus on preventing less mature attackers and detecting and responding to more mature attackers (see figure).

Based on this preliminary cyber threat assessment, the next step is to determine the scope of cyber security for your organisation and the underlying security capability model. The prevalence and sophistication of recent cyber-attacks on public and private organisations highlights a number of capabilities that are essential to becoming an effective cyber-resilient organisation:

- **Preparation:** prepare your organisation to effectively manage cyber risks by ensuring it has the right governance structures in place to enhance and maintain its preventative and detective security capabilities
- **Prevention:** defend your organisation against successful cyber-attacks by continuing to invest in enhancing and maintaining measures that protect your digital assets such as (i) next generation security controls (IDM, NAC, etc.), (ii) hardening of critical information infrastructure, (iii) secure services (secure SDLC, vulnerability and patch management, etc.) and (iv) secure workforce and cyber awareness
- **Detection:** leverage the wealth of threat intelligence and develop your own capabilities to ensure you are aware of the internal and external threats to your organisation and can pro-actively mitigate them
- **Response:** in anticipation of a cyber-attack, ensure you have the ability to rapidly respond to an incident in order to limit any adverse impact on your organisation

Figure 1



The five commandments for a successful cyber security strategy

In conclusion, five key principles should underpin cyber security and promote a cohesive approach to protection from cyber threats:

- **Understand your risk appetite:** only when you have fully understood your assets, the risks that threaten them and how these fit into the overall threat landscape can you determine what level of threat maturity you need to defend against and where you draw the line to focus on limiting the impact of a successful attack
- **Ensure close alignment with business goals:** ensure that your strategic direction for cyber security is in close alignment with business goals and the organisation's strategy for achieving these. Focus efforts on defending the most strategically important parts of the business, or those that carry most operational risk
- **Prepare for the worst:** it is not practical to prevent all forms of cyber-attack, especially those that are particularly sophisticated and targeted (advanced persistent threats or APTs). You should ensure you have the organisational and technical capability to rapidly detect and respond to a successful attack in order to limit its impact

Cyber resilience requires that organisations have the agility to prevent, detect and respond quickly and effectively, not just to incidents, but also to the consequences of the incidents

- **Share intelligence:** collaborate and share intelligence with industry and national and international cyber threat intelligence organisations. By sharing intelligence with other organisations you will be in a position to receive the benefit of shared wisdom
- **Instil a broad awareness of cyber security:** your security is only as strong as the weakest link. Ensure that the risks associated with cyber security and the steps your organisation is taking to combat these risks are understood across the organisation, from the board and senior management, to all staff, partners and third parties

Contacts

Editorial committee

Joël Vanoverschelde
Partner - Advisory & Consulting Leader
EU Institutions and Supranationals Leader
+352 451 452 850 - jvanoverschelde@deloitte.lu

Pascal Martino
Director - Strategy & Corporate Finance
+352 451 452 119
pamartino@deloitte.lu

CEO & CFO services

Benjamin Collette
Partner - Strategy & Corporate Finance Leader
+352 451 452 809
bcollette@deloitte.lu

Petra Hazenberg
Partner - Strategy & Corporate Finance
+352 451 452 689
phazenberg@deloitte.lu

Pierre Masset
Partner - CFA-Corporate Finance Advisory Services
+352 451 452 756
pmasset@deloitte.lu

COO & CHRO services

Basil Sommerfeld
Partner - Operations & Human Capital Leader
+352 451 452 646
bsommerfeld@deloitte.lu

Pascal Eber
Partner - Services Operations and
Excellence & Infrastructure Operations
+352 451 452 649 - peber@deloitte.lu

Filip Gilbert
Partner - Human Capital-Strategic Human Ressources
+352 451 452 743
fgilbert@deloitte.lu

CIO services

Patrick Laurent
Partner - Technology & Enterprise Applications
+352 451 454 170
palaurent@deloitte.lu

Jean-Pierre Maissin
Partner - Technology & Enterprise Applications
+352 451 452 834
jpmaissin@deloitte.lu

Stéphane Hurtaud
Partner - Information & Technology Risk
+352 451 454 434
shurtaud@deloitte.lu

CCO/CISO/CRO/CIA/BOD services

Laurent Berliner
Partner - EMEA Financial Services Industry
Enterprise Risk Services Leader
+352 451 452 328 - lberliner@deloitte.lu

Roland Bastin
Partner - Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu

Marco Lichtfous
Partner - Capital Markets/Financial Risk
+352 451 454 876
mlichtfous@deloitte.lu

Bank and Credit Institutions

Martin Flaunet
Partner - Bank & Credit Institutions Leader
+352 451 452 334
mflaunet@deloitte.lu

Healthcare

Luc Brucher
Partner - Healthcare Leader
+352 451 454 704
lbrucher@deloitte.lu

Insurance

Thierry Flamand
Partner - Insurance Leader
+352 451 454 920
tflamand@deloitte.lu

Investment Funds and Hedge Funds

Johnny Yip
Partner - Investment Funds and Hedge Funds Leader
+352 451 452 489
jyiplanyan@deloitte.lu

Technology, media and Telecommunications - Public Sector

Georges Kioes
Partner - Technology, Media &
Telecommunications and Public Sector Leader
+352 451 452 249 - gkioes@deloitte.lu

PSF

Stéphane Césari
Partner - PSF Leader
+352 451 452 487
scesari@deloitte.lu

Private Equity - Real Estate

Benjamin Lam
Partner - PE/RE Leader
+352 451 452 429
blam@deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg