

Inside

Quarterly insights from Deloitte, issue 7, 2015

CCO
CISO
CRO
CIA
BOD

LUXEMBOURG

EDITION
2 0 1 5



Top 10 for 2015—Our outlook for financial markets regulation

Global Director 360—Growth from all Directions

Developing an effective governance operating model—A guide for financial services boards and management teams

Aligning risk and the pursuit of shareholder value

Funds Transfer Pricing—A gateway to enhanced business performance

Small and Medium Enterprises in a globalised, post-crisis world—Reacting to new treasury risks and challenges with cash pooling solutions

Adopting a risk intelligent approach to pricing and capital needs for depositaries

Operational risk—An emerging focus for investment managers

Global Cyber Executive Briefing—Lessons from the front line

Cyber Insurance as one element of the Cyber risk management strategy

Becoming 'Reactively Proactive'—Rethinking compliance risk management in today's environment

FATF Guidance—Transparency and beneficial ownership

How to make financial crime prevention pay-off—Implementation strategies to reap the benefits of the holistic model

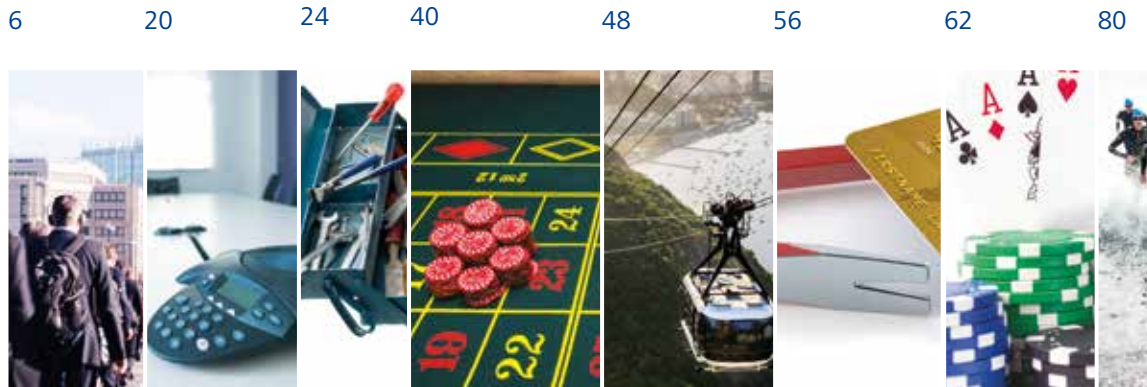
Positioning the internal audit function within the Solvency II framework—Key challenges

Risk appetite and assurance—Do you know your limits?

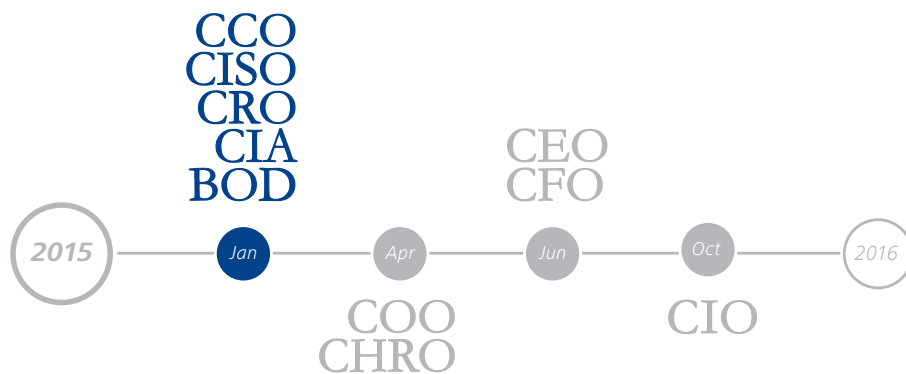
Managing social media risks to reputation risk—A hot topic on the board agenda

Deloitte.

In this issue



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



88

92

98

104

110

120

130

136



<p>4 Foreword</p> <p>5 Editorial</p> <p>6 Top 10 for 2015 Our outlook for financial markets regulation</p> <p>20 Global Director 360 Growth from all Directions</p> <p>24 Developing an effective governance operating model A guide for financial services boards and management teams</p> <p>40 Aligning risk and the pursuit of shareholder value</p> <p>48 Funds Transfer Pricing A gateway to enhanced business performance</p> <p>56 Small and Medium Enterprises in a globalised, post-crisis world Reacting to new treasury risks and challenges with cash pooling solutions</p> <p>62 Adopting a risk intelligent approach to pricing and capital needs for depositaries</p> <p>80 Operational risk An emerging focus for investment managers</p>	<p>86 Global Cyber Executive Briefing Lessons from the front line</p> <p>92 Cyber Insurance as one element of the Cyber risk management strategy</p> <p>98 Becoming 'Reactively Proactive' Rethinking compliance risk management in today's environment</p> <p>104 FATF Guidance Transparency and beneficial ownership</p> <p>110 How to make financial crime prevention pay-off Implementation strategies to reap the benefits of the holistic model</p> <p>120 Positioning the internal audit function within the Solvency II framework Key challenges</p> <p>130 Risk appetite and assurance Do you know your limits?</p> <p>136 Managing social media risks to reputation risk A hot topic on the board agenda</p> <p>142 Contacts</p>
--	---

Foreword



Dear readers,

2014 was a challenging year for the financial services industry and we expect that also this year will require innovative responses from all of us. 2015 will thus call for the same level of vigilance. Once more, the Inside team is very pleased to provide you with quarterly insights on hot topics catching the market's attention.

Like each year since 1971, January hosts the annual meeting of the World Economic Forum in Davos. The general assumption that a 'new global context for decision-making' is emerging is at the very top of the leaders' agenda. The world and the environment in which decisions are made are experiencing profound transformations. Consequently, new risks appear, old ones are changing - and the ability to cleverly understand and manage risks will be crucial. Thus, one year after the last governance, risk management & compliance edition of *Inside*, this first issue of 2015 points out key topics in these areas. It focuses on the roles and challenges of Boards of Directors, Board Committees, Chief Risk Officers, Chief Information Security Officers, Chief Compliance Officers, Chief Internal Auditors and Chief Actuary Officers.

With this new issue, *Inside* has reached its seventh edition! The growth and success of this magazine would never have happened without you, our faithful readers and contributors. 2015 is going to be promising for our magazine, which is even going global. This governance, risk management & compliance edition gives us the opportunity to launch a global version, led by Scott Baret (Global Financial Services Industry – Enterprise Risk Services Leader) and Laurent Berliner (EMEA Financial Services Industry – Enterprise Risk Services Leader). In this context, we are pleased to welcome more and more international contributors from the Deloitte network and we thank them for their enthusiasm and invaluable views.

This magazine embodies our strong conviction that the strength of our firm comes from its international dimension, favouring the diversity of views and reflexions able to grasp the complexity of today's world.

We hope you will find this publication insightful.

Joël Vanoverschelde
Partner
Advisory & Consulting Leader
Deloitte Luxembourg

Pascal Martino
Partner
Strategy, Regulatory
& Corporate Finance
Deloitte Luxembourg

Benjamin Hiver
Consultant
Operations Excellence
& Human Capital
Deloitte Luxembourg

Questions, feedback, comments?

Write to the *Inside* team:
luinside@deloitte.com

Editorial

Dear readers,

Welcome to this seventh edition of *Inside*, a publication dedicated to governing bodies and internal control functions. Our objective is to provide you with thoughtful insights on critical topics that may impact your organisation.

One such topic is regulatory pressure, which will likely remain very high and, in many industries, is not expected to ease in the foreseeable future. This creates challenges, but also opportunities for companies that adequately turn compliance with new requirements into competitive advantage. In this context, complying with regulatory requirements and good market practices are among the top priorities of companies' boards of directors, who seek to establish sound internal governance frameworks and 'governance cultures' that ensure authorised management and internal control functions give boards a clear and regular set of reporting that promotes adequate governance oversight.

The financial services industry, in particular, faces an unprecedented wave of interconnected regulations, including: structural reform and resolution in the banking sector; the data and regulatory reporting challenge; the forthcoming Capital Markets Union; and the approaching go-live date for Solvency II in the insurance industry. A new prudential scheme is emerging to encourage single-rules-book generalisation across EU countries, leading to the implementation of equivalent market practices. Banks are increasingly scrutinised by national regulators, as well as public and supranational authorities, in order to ensure appropriate monitoring of their risk appetites and stress-testing programmes. Our 2015 regulatory outlook sheds further light on these topics and many others. The main challenge for the financial services industry will be finding the right mix between compliance, risk management and financial performance.

The need to embed regulatory and risk management considerations into the strategic decision processes of organisations becomes a critical element of each organisation's success and performance, with the ultimate goal of creating shareholder value. In this regard, it becomes critical to align risk with the pursuit of shareholder value through the application of a risk-transformation approach. All industries are looking to enhance their performance by adjusting and adapting their risk models and approaches.

Fund transfer pricing for banks is a good way to capture all risks in the pricing of the transaction, allowing the transfer of costs from central treasury functions to the product originating those costs and related risks. In the same vein, the Alternative Investment Fund Managers Directive (AIFMD) regime imposes depositaries to rethink their capital adequacy assessments and, ultimately, the pricing applicable to their clients. These trends can be observed in organisations of all sizes, with small- and medium-sized enterprises seeking to optimize the management of their treasury through the development of cash pooling solutions to address treasury risks. With risk-based decision-making processes becoming central in today's business environment, a sound and complete identification of risks that companies may face is needed.

Risk can take various forms, and the evolving complexity of transactions and development of new technologies are causing new risks to emerge. In this regard, operational risks—such as cyber risk, model risk, or anti-money laundering (AML) risk—represent emerging priorities among many organisations. For instance, the recent introduction by the Financial Action Task Force (FATF) offers specific guidance on transparency and beneficial ownership in a context where undercover criminal activity—ranging from fraud and corruption to money laundering and tax evasion—tends to increase in the current, difficult economic environment. Another fundamental trend is the growing prevalence of social media that increases exposure to reputation risks and calls for a careful treatment by organisations, notably through their risk-appetite frameworks.

In such an increasingly complex environment, the internal audit function—perhaps more than ever—is a key actor within the organisation, providing comfort and assurance to governing bodies in terms of compliance with regulatory requirements and the adequacy of the risk-appetite framework.

These topics are covered in more details in this edition. We hope you enjoy reading it.

Sincerely,



Laurent Berliner
Partner
EMEA Enterprise Risk Services Leader
Financial Services
Deloitte Luxembourg



Bertrand Parfait
Senior Manager
Governance, Risk & Compliance
Deloitte Luxembourg



Please contact:

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

Bertrand Parfait
Senior Manager
Governance Risk & Compliance
Tel: +352 451 452 940
bparfait@deloitte.lu

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

Top 10 for 2015

Our outlook for financial markets regulation

David Strachan
Partner
European Center for Regulatory Strategy
Deloitte UK

Will 2015 be the turning point in the post-crisis regulatory agenda, when the focus shifts from repairing balance sheets and reputations to the role of financial services in promoting jobs and growth? And from proposing new rules to implementing the multitude already agreed over the last few years?

There are grounds for cautious optimism. On the banking front, the vast majority of the new primary requirements are now in place (with the important exception of EU bank structural reform), although there are still reviews of various elements of the existing capital framework and a significant amount of implementing detail to follow. After a very lengthy gestation, preparations for Solvency II will enter their final year. The new European Commission and

Parliament will push ahead with work to decide what falls under the umbrella of the Capital Markets Union (CMU). Recognition of the need for capital markets and non-bank finance to contribute to the jobs and growth agenda could influence the approach that would otherwise have been taken to deal with concerns about shadow banking. Indeed, the Financial Stability Board (FSB) now speaks about 'transforming shadow banking' into 'resilient market-based finance.'





There will be new institutions making a fresh start and they will be determined to make their presence felt. The European Central Bank (ECB) via the Single Supervisory Mechanism (SSM) has taken over as the prudential supervisor of eurozone banks. The new Single Resolution Board (SRB) will look at the resolvability of the cross-border eurozone banks, informed by the lessons learned from the FSB's first set of resolvability assessments for Global Systemically Important Banks (G-SIBs).

But there are clouds, some quite ominous, on the horizon. Standards and expectations have risen enormously across the board for all financial services firms - whether in terms of capital, liquidity, risk management or culture - and financial, as well as other penalties for transgressions seem to be rising inexorably. The effects of this will continue to be felt, for instance through the 'de-risking' which has been prompted by a number of Anti-Money Laundering (AML) and sanctions-related enforcement cases, with some institutions reassessing their risk appetites and exiting certain markets. Despite some aspects having been closed, residual enforcement actions by regulators, law enforcement agencies and competition authorities

in relation to London interbank offered rate (LIBOR) and FX benchmarks appear to have some way to go, and some of the behaviour revealed has reignited concerns about governance, culture and the structure of remuneration. Further, even if the balance is shifting from policy formulation to action and implementation, regulation will continue to occupy significant resources and senior management time, including building relationships with the new institutions. In particular, although primary legislation is in place for most of the new EU regulations and directives initiated by the last European Commission and Parliament, the European Supervisory Authorities (ESAs) still have to publish a formidable amount of detailed implementing standards. There will be plenty of devils lurking in these details.

Against this background, and regardless of whether 2015 is a year of relative brightness or darkness, firms will have to take some key strategic and business model decisions about which activities and products remain viable in a world of new multiple regulatory constraints on balance sheets. In many cases, the finalisation of requirements will crystallise the need for action. Banks will be most affected, but Solvency II will raise similar questions for some insurers.

This new regulatory environment will create opportunities and challenges both for incumbents and newcomers. Set against that, digital innovation will be a potent force, with the potential to transform the financial services landscape and define the winners and losers. Accompanying this opportunity is the threat of cyber-attack. For the board and senior management teams, all this puts an even greater premium on the clarity and rigour of their scenario analysis and contingency planning, underpinned by high quality data and timely decision-taking. In a world where firms may more readily be allowed to fail, and with 'challengers' knocking at many doors, agility and forward-thinking will be key.

1. Structural reform and resolution in the financial sector

Requirements for banks to ring-fence some of their activities have been debated for several years, but relatively little progress on implementation has been demanded. In 2015, this will change. In the UK, the largest banks must, in January, submit preliminary plans for how they will implement ring fencing. The largest foreign banks operating in the U.S. are required to submit plans for the implementation of Intermediate Holding Company structures. Banks in scope of domestic structural reform requirements in France and Belgium also face important deadlines. Planning is not easy; supervisors will expect banks to demonstrate a thorough understanding of their objectives and requirements and a credible strategy. But lack of planning will not be deemed acceptable.

Restructuring to meet authorities' expectations of resolvability will also be important. The initial results of the FSB's Resolvability Assessment Process (RAP) were published at the end of 2014, providing the first assessment of the progress that has been made to date by 10 out of the 30 G SIBs (the remainder will be reviewed by mid 2015). The FSB notes that although some G SIBs are making their legal entity structures less complex, further structural and operational changes may be needed. We expect that booking models will need to adjust and there will be a continuing focus on operational continuity for functions judged to be critical. There is also important unfinished business for some governments in terms of putting new resolution legislation in place. Next year will also see a second wave of filings of Recovery and Resolution Plans (RRPs) by banks in the U.S., where regulators took a tough line in 2014.



Resolvability planning will get underway in the EU as the Bank Recovery and Resolution Directive (BRRD) takes effect and the SRB starts to operate. Combining ring-fencing and resolvability considerations will add a layer of complexity to the strategic challenge for banks. Banks will need to consider how other rules (including OTC derivatives reform) and supervisory policies (such as increasing scrutiny of intra group transactions) play into their analysis.

Against this background, significant uncertainty hangs over EU requirements for bank structural reform. Proposals unveiled in January 2014 are proving contentious and are expected to remain so as the European parliamentary process continues. Fundamental questions remain unresolved and some will (continue to) argue that the proposal is unnecessary for structures that are indeed resolvable. But the proposal is unlikely to be withdrawn, although the derogation for national frameworks looks under threat. All this makes planning very difficult, yet domestic legislative timetables in some countries will force banks to take some decisions now. The key will be to do so in a way that retains some flexibility to make future adjustments.

It is not only banks facing resolution requirements. Financial market infrastructures and some insurers also face similar questions. The European Commission continues to work on its framework for Central Counterparty (CCP) resolution, which the new Commissioner for financial services has said will be 'one of [his] first priorities'. CCPs will also be faced with a new international disclosure standard, and it has even been suggested that a new loss-absorbency requirement could be looked at, although it is unclear how such a requirement would be translated from banks to CCPs.

Banks will need to consider how other rules and supervisory policies play into their analysis

At the international level, Global Systemically Important Insurers (G-SIIs) were originally expected to have RRRPs in place by end-2014, although the FSB's RAP report makes it clear that this timetable has been extended.

The FSB has set out an ambitious work programme on insurance resolution for 2015, although it is still far from clear how much effort national authorities will put into this and, eventually, how much structural change emerges. One acid test will be the speed with which national authorities look to incorporate the FSB's key attributes for the effective resolution of insurers into their domestic legislation.

2. New institutions in action

2014 saw important institutional changes in the EU. In 2015, the implications for financial services will begin to play out. A new guard in the European Commission and Parliament, for the first time since the financial crisis, may dedicate a larger share of the financial services agenda to promoting growth through alternatives to bank financing than to the 'safety and soundness' considerations that dominated their predecessors' work. A similar change in emphasis was signalled by Mark Carney, chair of the FSB, after the recent G20 meeting.

In the EU, a new focus on non-bank forms of finance to promote jobs and growth and, as part of this the CMU, may moderate proposals for dealing with shadow banking. What happens on the proposed Money Market Funds (MMF) Regulation will give one early indication of how this balance will be struck. In the eurozone, the start of the SSM initiates a journey that will test banks and supervisors.

The ECB will work hard to instil a new supervisory culture and good practice across the region. It will be important for banks to engender dialogue, trust and a strong understanding of their business with supervisors.

New supervisory expectations will be important drivers of business strategy. We expect the first half of 2015 to be dominated by dealing with issues highlighted by the Comprehensive Assessment, with some of the more difficult or complex aspects informing longer-term supervisory actions. Consistency of risk-weighted assets and model validation will be important topics for thematic work by SSM supervisors in the coming year. More broadly, harmonising the discretions available to supervisory authorities across the eurozone is high on the ECB to-do list. The Supervisory Risk Evaluation Process (SREP) will become an increasingly important part of the dialogue between banks and supervisors.

The SRB, part of the Single Resolution Mechanism (SRM) within the Banking Union, remains an unknown quantity but will wield significant power. From January 2015, it will begin working with national authorities on resolution planning, resolvability assessments and the setting of loss absorbency. This new institution has received relatively little attention to date. However, given the significance of the SRB's influence, this needs to change in 2015.



3. Data and regulatory reporting

Appetite from supervisors for more granular data, has been growing since the start of financial crisis, but in the coming year several initiatives will combine to mean data and reporting are once again critical for firms. Although in the near term, cost and time pressures may force firms to adopt tactical solutions, in the longer run it could be more effective to take a view on more fundamental and strategic changes. And in some cases, supervisors may insist on a strategic solution.

Foremost in the minds of the largest Eurozone banks will be the follow-up to the asset quality review (AQR) completed as part of the ECB's Comprehensive Assessment. Many banks experienced difficulties providing accurate data in the form that supervisors wanted on a timely basis. The ECB will also introduce regulation on reporting of supervisory financial information.

Supervisors also expect banks to improve their risk data capabilities. Although the Basel Committee on Banking Supervision (BCBS)'s Principles for effective risk data aggregation and risk reporting currently only apply to G-SIBs, the indications are that supervisors will expect the principles to be adopted more widely. The G-SIBs have until 1 January 2016 to comply with the BCBS's principles and we expect 2015 to be a year of significant activity, with some banks finding it a challenge to make progress.

The challenge extends beyond risk and prudential data. The FSB recently observed that G-SIBs' management information systems may still not be capable of providing accurate or relevant information required in resolution in the right timeframe. In the EU, the European Banking Authority (EBA) is consulting on technical standards for the independent valuation that will be carried out in the event a bank is resolved.

Important changes are being made in accounting standards which, with time, are expected to affect prudential reporting and capital. For example, IFRS 9 provides new guidance on the classification and measurement of financial assets and introduces a new expected credit loss model for calculating impairment.

During 2015, banks will begin programmes of work expected to last at least two years, although the earliest reported financial impacts are expected to be in 2015 and 2016 ICAAPs.

Insurers will face more stringent data and reporting requirements as well which to a significant degree is driven by Solvency II transposition timelines. 2015 is the first year in which preparatory Pillar III reporting disclosures are expected prior to Solvency II implementation on 1 January 2016. Furthermore, Solvency II continues to present insurers with the significant challenge to source data to the right level of granularity, for example related to look-through asset data. Ensuring rapid access to the required data remains an industry issue. Building-in known elements of other upcoming data and reporting requirements (for example IFRS 4 Phase II or resolvability assessments) will minimise the need to 'dig up the road twice' when the new requirements come into play.

Regulators are also seeking to increase transparency in capital markets and shadow banking. Further detail will emerge next year from the European Securities and Markets Authority (ESMA) on the expanded post-trade reporting, transaction reporting and commodities derivatives position reporting requirements under the Markets in Financial Instruments Regulation (MiFIR). The regulation on reporting and transparency of securities financing transactions is also likely to enter into force next year.

Data protection reform in the EU, likely to be concluded in 2015, will be another important consideration in reforming data systems.

It will be important for banks to engender dialogue, trust and a strong understanding of their business with supervisors

4. Culture and treatment of customers

Culture and the treatment of customers will remain at the forefront of the financial services debate. Banking and capital markets activities are in focus following well-publicised transgressions (which in some cases continued into the second half of 2013), but the principles have broader relevance for all financial services sectors. There is no doubt about the seriousness of the crackdown on activities perceived to have the potential to lead to consumer detriment, whether retail or wholesale, or harm market integrity. Everyone in financial services can now talk culture, but the real challenge is to 'do' culture – identify it, articulate it and embed it at all levels of the organisation. This is where supervisors will expect to see hard evidence of significant progress in 2015.

In the UK, new Senior Managers Regimes are being introduced in both banking and insurance. This will result in more supervisory scrutiny of individuals in scope and (especially in banking) potentially significant individual liability if things go wrong. The PRA explicitly prescribed two responsibilities linked to culture (one for developing, the other for embedding culture), which should concentrate minds on this, as well recent enforcement action by the FCA. To prepare, the industry needs to focus on how senior management can best oversee culture and conduct risks, putting conduct risk MI high on the agenda. In 2015, the UK's BRSC will launch, with measuring improvements in banking culture and consumer outcomes high on its agenda.

In the EU, the ESAs have been encouraged to up their game on consumer protection across the EU, although it remains to be seen whether they can secure the additional budget and resources to make this a reality, with everything else they have on their plate. One area where they will be very busy with respect to investor protection will be in developing level two measures, in particular for the Markets in Financial Instruments Directive (MiFID II) and for the Regulation on Key Information Documents for Packaged Retail and Insurance-based Investment Products (PRIIPs).

Wholesale conduct issues will run well into 2015, and possibly beyond. The UK's FEMR will report in mid-2015, with its focus being on fixed-income, currency and commodity markets, and their associated derivatives and benchmarks. The review entrenches the idea that regulators will no longer wait for misconduct to materialise before taking action - the focus is on the susceptibility of markets to abuse, and taking preventative action.

This means action on systems and controls, but also behavioural practices, and the incentive systems which drive that behaviour. In our view it would be short-sighted to regard the outcome of the FEMR as only affecting the UK. Given the UK's role in global markets, what starts there is bound to have ramifications for other major financial centres.



5. Competition and innovation

From April 2015, in the UK the FCA and CMA will be 'concurrent' competition regulators for financial services. What this means in practice remains to be seen, and it may be some time before it is clear which authority takes the lead on what. At present, there are ongoing competition reviews by the FCA in a number of areas, while the CMA has recently launched a market investigation into personal current accounts and SME banking, due to report its provisional findings and possible remedies in September next year.

The new Payment Systems Regulator (PSR) (which will have a competition objective) will also take on its full responsibilities in April 2015, by when HM Treasury will have concluded its consultation on which systemically important payment systems come within its scope. With payment services at the forefront of digital innovation in banking the work of the PSR will be all the more important.

The PRA now also has a secondary objective to facilitate competition. While we do not expect the PRA to be as active in relation to competition issues as the FCA, competition considerations will be more prominent in its work that has previously been the case. Under the new competition framework, the FCA will be obliged to consider whether its competition law powers should be used before taking action in line with its regulatory powers.

The competition powers raise questions relevant across all financial services from cash savings accounts to retirement income products, from consumer credit activities to wholesale market activities. Over the course of 2015, the FCA will continue its programme of thematic reviews and market studies. The questions it is posing to the industry are granular and challenging, with supervisors delving into details of business lines to identify potential competition issues. The regulatory treatment of challenger banks and challenger products (such as potential successors to annuities) will bear watching closely, as regulators hope to spur innovation through the elimination of competitive distortions.

As a measure of progress to date, the PRA and FCA authorised five new banks between March 2013 and 2014 and have seen an increase in the number of firms discussing the possibility of becoming a bank. UK authorities are not alone in their competition focus. The new Commissioner for Financial Stability, Financial Services and Capital Markets Union, Lord Hill, seems to have taken a leaf out of Martin Wheatley's book by signalling that he will seek to put consumers at the centre of financial services policies through promoting competition, transparency, choice and innovation. Competition is also a significant motivation for revisions to EU payments legislation and for rules on non-discriminatory access to trading venues and CCPs contained in MiFIR.

Competition is also a significant motivation for revisions to EU payments legislation and for rules on non-discriminatory access to trading venues and CCPs contained in MiFIR

Much of the regulators' competition related work is likely to have implications for strategy and business models. While the impact may not be as stark as in the UK's payday lending industry, where charge caps will apply from the start of next year, there is a threat to profitability for some business activities for incumbents.

At the same time, increased competition will open up opportunities. In practice this means that all types of financial services firms will need to become more attuned to regulators in the widest sense looking at their activities through the lens of competition. And while many organisations will bring these skills and perspectives to bear when dealing with competition authorities, they will be less prevalent in compliance and risk management functions when they are dealing with 'traditional' financial services regulators.

This needs to change.

6. Stress testing and risk management

For banks, 2014 saw unprecedented activity in stress testing, underscoring the importance supervisors now give to it as a diagnostic and risk management tool. Stress testing is becoming more frequent, more invasive and more demanding. And it is not just a concern for the largest banks; the same principles are likely to be applied (proportionately) to others.

Some banks involved in the ECB's Comprehensive Assessment, which incorporated the EBA's stress test, will have significant remediation work to do as a result of identified shortcomings in data and processes. Although the ECB has indicated it is unlikely there will be a repeat of the EBA exercise in 2015, it is equally likely there will be one in 2016. At least as important will be the role of stress testing in the ECB's individual capital and liquidity assessment processes. We expect over time, the approach to more closely resemble the style of the Bank of England's (BoE) framework for Pillar 2 stress testing.

At the same time, as stress testing exercises become more challenging from a risk perspective, supervisors will also place greater emphasis on banks' stress testing processes and governance. There will be marks for showing your workings as well as for the final result.

Between them, the ECB, BoE and U.S. Federal Reserve (which also has its own stress testing framework) are responsible for the supervision of 21 out of 30 G-SIBs. Several G-SIBs will be subject to two sets of stress tests and a handful to all three. These banks need to identify what synergies exist. Supervisors will look at the consistency between a bank's internal stress testing, assumptions made in recovery and contingency planning, and (if separate) in the SREP. Strong controls and oversight will be required to achieve that consistency.

This means that tactical approaches to supervisory stress testing, often divergent from banks' own stress testing exercises, will ultimately not be sustainable (nor permitted by supervisors). It is much too early to talk of an international consensus on an approach to stress testing, but there may be scope to identify areas of alignment, especially as authorities become more comfortable with their own tests.

Ultimately banks should recognise that, in the context of a forward looking, judgement led approach to supervision, scenario analysis and stress testing are key supervisory tools. They will not just be the marginal determinant of capital in future, but also an important driver of the whole supervisory dialogue.

Regulators in each jurisdiction may watch nervously for any signs of post-crisis regulatory reforms being unpicked as part of the wider negotiations

7. Capital Markets Union

Capital Markets Union (CMU) is a flagship initiative for the new European Commission with a rapidly developing agenda and potentially a very broad scope. The primary motivations are to increase jobs and economic growth, and to develop a more resilient financial system. In contrast to the Banking Union, it will apply to the whole of the EU and seeks to facilitate the growth of new markets. That will be achieved by increasing market-based funding, lowering the cost of raising capital and eliminating barriers to the cross-border provision of financing, particularly for Small and Medium-sized Enterprises (SMEs).

The revival of transparent and simple securitisation markets and the development of EU private placements markets are seen as key. More broadly, CMU has in scope the various initiatives that have previously been pursued as part of the shadow banking agenda. However, its scope is potentially very wide and expands beyond regulation to areas such as financial reporting, insolvency law and tax.

The CMU agenda will need to maintain a balance between policy seeking to facilitate growth and regulation to ensure financial stability and investor protection. Important questions remain about what progress on the CMU will entail, including the implications for the remit of ESMA and for the Level 2 development of key capital market regulations such as MiFID II/MiFIR, and existing regulations such as the Prospectus Directive, Market Abuse Directive (MAD II) and the Transparency Directive. Integration of the CMU action plan with current initiatives will be a key to the success of the development of a CMU.

Although Lord Hill has made it clear that he expects new legislative proposals only to be produced after careful analysis of the current impediments to CMU, history suggests that there will be no shortage of ideas for bold new initiatives. Indeed, some of the debate echoes discussions which took place decades ago. That said, there is an opportunity for market practitioners, with direct experience of what does and does not work in the EU's capital markets today, to shape this agenda. If they do not, others are likely to.



8. Business model mix in a world of multiple constraints

As banks roll out changes to meet the requirements of Basel III, the strategic challenge will turn to managing the implications. High amongst those is what business model and mix of activities, banks will pursue once the regulatory constraints are in place (capital, liquidity and leverage ratios, stress testing) and loss absorbency requirements are taken into account. Determining which business lines are most profitable and in what combination is increasingly complex.

Some of these requirements are now set, although there remains uncertainty about others, for example, in the case of the FSB's recent consultation on Total Loss-Absorbing Capacity (TLAC) - the minimum calibration, the use of Pillar 2 and the ability of host authorities to call for additional TLAC to be held in subsidiaries (as well as how requirements will be implemented in the EU). There is also uncertainty on the outcomes of the BCBS's proposals on the Fundamental Review of the Trading Book and its reviews of the standardised approach to credit risk, interest rate risk in the banking book and capital requirements for operational risk.

Although a standard has been agreed internationally for the leverage ratio, the calibration of a minimum requirement remains to be decided.

Notwithstanding these uncertainties, there is no reason for banks to delay building the capabilities they need to manage their balance sheets in this much more complicated regulatory environment and to take decisions on the right business model mix. Divining an optimal strategy that considers all metrics simultaneously and at different points of the economic cycle (when different constraints may bind) will present a significant challenge.

The need for individual banks to invest in this capability will depend significantly on their business models, with the G-SIBs likely to be most significantly affected - not only because of the nature of their activities, but also because of the trend by many supervisors across the world to require the localisation of financial resources. This complicates capital and liquidity management by reducing the flexibility and fungibility of financial resources.



9. Solvency II and insurance capital

Preparations for Solvency II implementation will enter their final year in 2015, with the expected approval of the Delegated Acts in June 2015 being a key date in the finalisation of the regime. Completion of the asset data templates in the preparatory period and under the full regime remains a challenge for insurers.

Solvency II will also raise some questions for insurers in terms of business model mix, although the challenges will not be as acute as for banks. New capital requirements will affect the optimal asset allocation for insurers, and they will also have some important choices to make in relation to the various transitional provisions open to them. Again, this will require careful scenario analysis to inform initial decision, followed by careful monitoring to ensure that the firm is operating within the constraints of the option(s) chosen.

We expect those insurers applying for internal model approval to be subject to continuous scrutiny as applications are filed for approval, especially those regulated by the Prudential Regulations Authority (PRA). It is inevitable that some of the scepticism that the UK's banking supervisors are showing towards banks' internal models will rub off on their insurance counterparts. As part of this, model governance arrangements, including the role and responsibility of non-executive directors, will be tested.

While Solvency II is a maximum harmonising Directive, concerns over a level playing field for EU insurers are unlikely to be addressed with the transposition of the Directive in 2015. Much will depend on how the transposed rules are applied by local supervisors and convergence of supervisory approaches will be a much longer process.

Meanwhile, at the international level work is gaining steam to develop a global Insurance Capital Standard (ICS) for G-SIIs and for Internationally Active Insurance Groups (IAIGs) as the insurance capital and resolution debate increasingly follows that in the banking industry. As a first step the International Association of Insurance Supervisors (IAIS) completed its work on the Basic Capital Requirement (BCR) in the autumn of 2014 and this will be used as the foundation for calculating Higher Loss Absorbency (HLA) for G-SIIs. It remains to be seen how much impact the global capital standards will have on G-SIIs and the wider insurance industry and the extent to which any G-SIIs will have to change their business mix or raise capital as a consequence.

For the G-SIIs, the bigger impact may in fact come from the increased intensity of supervision they attract and the extent to which this requires them to change their risk and capital management approaches.

Determining which business lines are most profitable and in what combination is increasingly complex



10. The interaction of market structures in different countries

Financial market structures are being radically altered by multiple regulatory requirements, and the way in which users of those markets interact with them is set to change as a result. Old issues of extraterritoriality have not yet gone away, and appear unlikely to any time soon, despite efforts at the international level to focus on equivalence of outcomes and deference to local rules.

2015 will likely see a key EU equivalence decision on U.S. derivatives rules and continued coordination to resolve cross border issues in the implementation of the derivatives reform agenda, with implications for the geography of derivatives trading. There will also be significant decisions made in relation to which categories of derivatives will face mandatory central clearing, with any inconsistencies between regions likely to spur banks to reassess where they book segments of their business. Supervisory scrutiny of booking models, including of remote booking and back to back intra group transactions for risk management purposes, looks set to continue. Overall, we expect to see more regionalisation of booking practices.

Meanwhile, the implementation of MiFID II/MiFIR will affect all stages of the life-cycle of a trade, from pre-trade transparency, through to execution, and ultimately reporting and other post-trade requirements. We can expect wrangling over the all-important technical details of the MiFID framework in the next two years, particularly as non-EEA investment firms face the prospect of enhanced wholesale market access if favourable equivalence decisions are made.

The intended effect of these regulatory changes is to bolster financial stability, including through increased transparency. Mandatory clearing, rigorous risk management standards for non cleared derivatives and greater use of trading venues will all contribute to this. However, the impact on liquidity and on the choice of derivatives available to end users is less clear, with the cost of non cleared derivatives set to increase significantly and the number of banks offering a full suite of such products reducing. Market liquidity more generally is under pressure as various new regulatory requirements are causing dealers to re-assess their ability to hold inventory and provide liquidity. In addition, the role of CCPs will become increasingly important, attracting attention not only from regulators and resolution authorities but also from CCP members and end users.

The politics of the Transatlantic Trade and Investment Pact (TTIP) are tricky, but TTIP remains one to watch, with EU officials continuing to push for financial regulation to be included, while U.S. authorities resist. Regulators in each jurisdiction may watch nervously for any signs of post-crisis regulatory reforms being unpicked as part of the wider negotiations.

We do not expect a fully evolved global market structure to emerge by the end of 2015, but the way that these forces are shaping market outcomes should be much clearer by then.

Supervisory scrutiny of booking models, including of remote booking and back to back intra group transactions for risk management purposes, looks set to continue

Global Director 360 Growth from all Directions

Dan Konigsburg
Managing Director
Global Center for Corporate
Governance and Public Policy
Deloitte Touche Tohmatsu Limited

Michael Rossen
Director
Global Center for Corporate
Governance
Deloitte Touche Tohmatsu Limited

Kevin Tracey
Business Program Specialist
Global Center for Corporate
Governance
Deloitte Touche Tohmatsu Limited

Boards around the world are changing.
So are corporate governance concerns
and boardroom responsibilities.
As markets have increasingly become more
interconnected, how are boards responding?



In the latest edition of our global corporate governance benchmarking survey, *Global Director 360°: Growth from all Directions*, we compiled the perspectives and insights of 317 boardroom directors at public and private companies across 15 countries and regions, including, for the first time, Luxembourg. We sought their input on a variety of timely 'hot topic' governance, regulatory and compliance concerns that companies around the world are facing.

The resulting image was that of a changing governance, regulatory and compliance landscape. The results reveal that the global financial crisis (the crisis) weighs less heavily on directors' minds and boards' agendas. Based on the survey responses, boards are becoming more confident that markets are emerging from the crisis.

Top boardroom issues

Only 20% of the global respondents cited the crisis as a top boardroom issue impacting their boards in the past 12 months. This represents a decrease of 23 percentage points from the prior edition - the largest decrease for any top issue year-over-year. It was the single most discussed boardroom issue highlighted in our last survey.

As to issues that are replacing the crisis in the minds of directors, 20% more global respondents are focusing on performance compared to our 2012 survey - the second most often discussed issue, behind strategy. Other topics gaining prominence in global boardrooms included growth (13% point increase) and shareholder value and investors (11% point increase).

These results may indicate that boards are focusing less on recovery from effects of the crisis and more on company performance and operations as well as on the creation of long-term sustainable growth - news that certainly is welcomed by investors globally.

In Luxembourg, we find that an overwhelming majority of boards (81%) discussed regulation, governance and compliance concerns - nearly double the rate of risk management and performance, the second and third most discussed topics in Luxembourg boardrooms, respectively. Directors in Luxembourg expect to be focusing on similar topics in the coming 12 to 24 months.



Cyber risks

Cyber security issues are still not being given sufficient attention by global organisations - nearly half (49%) of global boardroom directors (59% in Luxembourg) do not currently discuss cyber security risks as part of their technology agenda.

In addition, over a quarter (27%) of the global directors surveyed fail to discuss technology risks at all. In light of all the recent news surrounding security incidents and data breaches, it is surprising that we are not seeing an increased number of boards discuss the security risks facing their company. Failure to take preventative measures to protect against breaches in security poses a huge risk to organisations.

Such risks could potentially expose them to internal control deficiencies and reputational risks that may ultimately result in lost revenue. Luxembourg boards, however, appear to actively be discussing other technology risks at a higher level than their global counterparts - data privacy (71% vs. 57% globally) and international data transfer (42% vs. 21%), to name a few.

Social media

Nearly two-thirds of all directors surveyed globally (and nearly three-quarters in Luxembourg) stated that their board does not use social media. This result is a bit surprising, and raises potential questions: as the world moves towards an increasingly digitised environment, are boards fully prepared to deal with the unprecedented business and reputational risks their organisations face? Are boards equipped to monitor and engage with their evolving stakeholders?

Many social media sites and tools have appeared only in the past decade, and perhaps knowledge and understanding of these tools have not yet reached the boardroom.

On the other hand, some directors are already embracing this new technology, understanding its impact on the organisation. It is plausible, however, that directors may be wary of regulatory compliance concerns related to disclosing sensitive corporate information via social media or may not yet view the use of social media as relevant to their responsibilities.

Shareholder engagement

Our survey found shareholder engagement to be a topic of interest. Going forward in this post-crisis environment, investors and other stakeholders can be expected to closely monitor board activities.

Indeed, nearly 70% of global respondents expect the level of interaction between shareholders and boards to increase over the next few years. It would thus seem reasonable to assume that engaging with investors would be a priority for directors. Yet our survey results indicate that despite acknowledging increasing levels of shareholder scrutiny, 61% of the global respondents noted that they have not developed and implemented a shareholder engagement policy.

The number was even higher in Luxembourg (75%). As scrutiny and activism continue to evolve, boards are likely to develop more structured and practical ways of engaging more frequently and closely with their investors and relevant activists.

Diversity

On the topic of boardroom diversity, some countries have enacted regulations or legislation to increase the presence of women, while in other countries organisations have implemented their own related initiatives or policies. In our survey, nearly two-thirds of global respondents indicated that their organisations have not introduced diversity policies for board composition; Luxembourg directors reported higher numbers.

Only 20% of the global respondents cited the crisis as a top boardroom issue impacting their boards in the past 12 months

One obstacle to greater diversity could be the long tenure of directors and the lack of term limits or age limits on board service. Our findings show that 62% of global directors surveyed indicated that their boards have not implemented term or age limits, or that they were unsure whether they have such limits. Boards appear to be implementing term limits for director service (30%) almost twice as frequently as age limits (17%). These global results do not vary significantly from the Luxembourg situation. Globally, it appears that, while good progress is being made in improving diversity in the boardroom, there is still a long way to go before we will see significant change in terms of numbers.

Looking onwards

The decreasing levels of concern over the crisis may indicate that directors around the world see the struggles related to the crisis and its aftermath as finally behind them. This should free up time, attention and other resources, allowing boards to focus on assisting their organisations in achieving long-term growth.

Directors' ability to contribute to and oversee management's performance as well as the organisation's strategic direction should be keys to success as companies look beyond the constraints that have hemmed them in over the past several years.

Developing an effective governance operating model

A guide for financial services boards and management teams

Scott Baret
Partner
Deloitte US
Global Enterprise Risk Services Leader
Financial Services
Deloitte Touche Tohmatsu Limited

Edward T. Hida II, CFA
Partner
Global Leader - Risk & Capital
Management
Global Financial Services Industry
Deloitte US

Nicole Sandford
Partner
National Practice Leader
of Governance Services
Deloitte US



A governance operating model is the mechanism used by the board and management to translate the elements of the governance framework and policies into practices, procedures, and job responsibilities within the corporate governance infrastructure



Introduction

In recent years, many boards of directors in the financial services industry (FSI) have been working to bolster the effectiveness of their organisations' governance models. For example, boards appear to have strengthened their governance frameworks and policies and reasserted their governance roles, established board-level risk committees, clarified the responsibilities of other board committees, and appointed chief risk officers (CROs) or reinforced the independence of existing CROs. Concurrently, senior executive teams have committed resources to enhancing governance frameworks.

However, many FSI companies may have come to realise that work remains if they are to operationalise the structures and institutionalise the principles they have adopted. Moreover, the expectations of regulators, investors, and other stakeholders regarding governance have shifted over the past few years (see sidebar: Drivers and expectations). Stakeholders now see boards as more accountable for the effectiveness of their overall governance process. This shift is real, and it is significant, and is likely to amount to an expectation of greater board involvement in the means by which governance is organised and effected, and for more **active oversight** by the board and its committees.

Greater involvement and more active oversight may be evident, but governance is also a work in progress, as reflected in Deloitte's experience and research. A Deloitte review of bank board risk committee charters found that board members "*want to clearly identify areas in which they are responsible for approval of decisions; where others (usually, senior executives) are responsible for approval decisions that they must as board members oversee, further approve, or simply be aware of; and how.*" A governance operating model supplies the "*how*"¹ that board members seek and can reveal gaps or shortcomings in board or management committee charters.

A Deloitte study of disclosures in proxy statements found that while FSI companies are bolstering governance and oversight, only 33% of those surveyed have

management risk committees, 41% disclose whether risk management/oversight is aligned with strategy, and 19% note the board's oversight with regard to corporate culture.² The trend toward increasing disclosure regarding governance and risk oversight implies a need for reliable methods of operationalising governance.

While the board is accountable for oversight of the governance process, management is responsible for implementing the policies and procedures through which governance occurs within the organisation. The board is responsible for understanding—and for advising management on—the processes through which governance occurs within the organisation, and is accountable for the results of those processes. Management is responsible for the governance processes and their workings, and for their results.

A **governance operating** model may assist the board and management in fulfilling their governance roles. Such a model is likely to enable the board and the executive leadership to organise the governance structure and the mechanisms by which governance is implemented. By the same token, the lack of a governance operating model may lead to an incomplete or faulty governance structure, or to inconsistencies, overlaps, and gaps among governance mechanisms. Such inadequacies may lead to failure to enact governance policies that the board and management have put in place.

The sheer complexity of governance and the huge number of related procedures and other mechanisms in a global financial institution may indicate a need for a governance operating model. The elements of such a model may exist within many large FSI companies. However, those elements may not have been connected, rationalised, and organised to provide the consistent guidance and incentives that executives, risk managers, and business unit leaders require. A governance operating model has the potential to address this need and thus enhance management's ability to implement governance and the board's ability to exercise proper oversight.

1 *Improving Bank Board Governance: The bank board member's guide to risk management oversight*, Deloitte Center for Financial Services, 2011, deloitte.com <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/FSI/US_FSI_ImprovingBankBoardGovernance_122911.pdf>
2 *Risk Intelligent proxy disclosures – 2011: Have risk-oversight practices improved?*, Deloitte Center for Corporate Governance, 2011, HYPERLINK "<http://www.deloitte.com>" deloitte.com <http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/IreEng/Page%20Copy/Home/Risk%20Intelligent%20Proxy%20Disclosures%202011_Deloitte_083011.pdf>

Drivers and expectations

Three main drivers familiar to FSI leaders have likely intensified the need for improved governance: the growth imperative, organisational size and complexity, and regulatory change.

- **Growth must continue.** Customers, investors, and the public recognise that a sound, robust, competitive financial services sector is a key component of a healthy economy. Customers want products and services, and investors want returns; meanwhile, regulators and the public want accountability, responsibility, safety, and soundness in institutions and the financial system. Balancing these desires calls for FSI companies that can grow within the purview of sound governance
- **Size and complexity are permanent.** While the debate about whether financial institutions are “*too big to fail*” continues, many are significantly larger than they were before 2008. For the largest firms, global reach is a reality, as is complexity of products, markets, and regulations. Given this, boards should consider reliable methods of enabling executives and managers to implement governance
- **Regulations have proliferated.** In response to the financial turbulence of the past years, many regulatory agencies and advisory groups have issued guidance relevant to board governance. Yet regulatory change and lapses in governance are likely to continue. This indicates a potential need to extend the governance process deeper into the organisation

Coupled with governance and risk management lapses before and since the downturn, these drivers have likely shaped regulators’ and other stakeholders’ expectations in the following ways:

- The board’s governance role includes responsibility for reviewing corporate strategies, shaping the culture, setting the tone at the top, and promulgating the organisation’s vision, values, and core beliefs
- The board is expected to oversee senior management’s collective ownership and individual accountability for regulatory compliance and risk management
- The board should attain enough visibility into business operations, processes, and risks to understand the risks management is taking and how they are being managed
- The board is accountable for all aspects of governance, including:
 - Decision-making authority that codifies who is responsible for making key decisions
 - Organisational structures that define and clarify responsibilities for operational, control, and reporting processes
 - Organisational design that is understood by managers, employees, and external stakeholders

Although many FSI companies may have responded to these drivers and expectations (for example, by developing committee structures and establishing policies), they may still be grappling with operationalizing governance. A governance operating model could potentially assist in addressing this challenge.

This document, prepared for board members, board committee members, senior executives, and risk managers at FSI companies, aims to assist boards and others with key governance roles in developing a robust governance operating model. This document also provides suggestions to consider on how to begin implementation, although that is not its primary focus. Such a model may foster the information flows and visibility into processes that enable both the board and management to fulfill their respective governance responsibilities. For FSI companies with a governance framework and policies in place, this document

outlines a next step—moving governance to the level of people’s day-to-day job responsibilities.

This document assumes that readers are broadly familiar with recent FSI regulatory developments and with key principles of governance, including those Deloitte has identified over the past several years in documents such as *Risk Intelligent Governance: A Practical Guide for Boards: Improving Bank Board Governance*, and *The Risk Committee Resource Guide for Boards*.³

³ Each of these documents is available at deloitte.com.

Figure 1 depicts the major components of a governance operating model and their relationship. This high-level view shows the major components—structure, oversight responsibilities, talent and culture, and infrastructure—and their key subcomponents. The nuts and bolts of the model (layers below the subcomponents in this depiction) include process flows, procedures, and reporting mechanisms that implement governance at the level of job responsibilities. Board and management choices regarding each component should define how the governance operating model will be implemented by management.

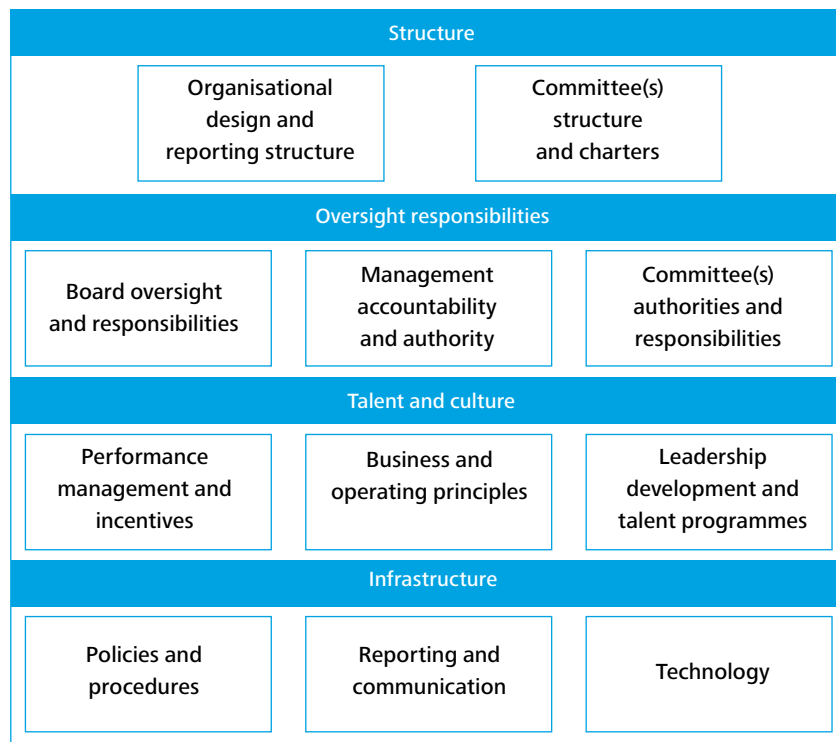
- Bring the organisation’s governance framework down to the level of roles, responsibilities, reporting lines, and communications to bridge the gap between the governance framework (discussed in the following section) and operational realities
- Help people to answer questions such as, “Why are we doing this?” “Is this okay?” “Whose call is this?” and “Who do we need to tell about this?” and to know when to ask such questions
- Sustain governance by creating a feedback loop in which the board and management can identify and respond to new business, operational, competitive, and regulatory needs

In practice, a governance operating model should:

- Organise operational, financial, risk management, and reporting processes such that the board receives the information it requires to effect good governance and management and the business units can conduct their activities in ways that comply with regulations and serve strategic ends

A governance operating model may contribute to solving the common problem of ‘management by memo’ in governance. It is rarely enough for the board or management simply to articulate principles and issue policies, no matter how clearly and forcefully they do so. They should also see to it that people have the understanding, motivation, and means to implement them, and that they do so.

Figure1: Illustrative governance operating model



Copyright © 2013 Deloitte Development LLC. All rights reserved.

From framework to operating model

The starting point, which many FSI companies have likely addressed, is the governance framework, such as that developed by Deloitte or another organisation. The Deloitte Governance Framework (Fig. 2) was developed to help boards and executives assess their organisations' governance programmes.

Whether the board and management adopt or develop a governance framework, it articulates the various elements of the governance programme, clarifies the governance roles of the board and management, and illustrates an appropriate relationship between governance, risk management, and organisational culture.

Figure 2: Deloitte governance framework



Copyright © 2013 Deloitte Development LLC. All rights reserved.

The overarching benefit of a sound governance operating model is that it could enable the board and its committees to execute their responsibilities properly and with greater assurance that they have done so

Encircling all elements of the framework is the corporate governance infrastructure. The governance infrastructure is the collection of governance operating models—the people, processes, and systems—that management has put in place to govern day-to-day organisational activities. This infrastructure also includes the processes used to gather and report information to the board and external stakeholders, as well as to management.

The board's role in various elements of the governance infrastructure ranges from overseer to active participant in the actual processes. The top half of the framework above depicts areas where the board's responsibility is typically heightened. In these areas, it is generally not considered adequate for the board only to understand and monitor the company's operating models; in addition, the board will be expected to play a role in developing the components and participating in the activities.

These areas include governance (here meaning the board's structure and composition), strategy, performance, integrity, talent, and risk governance. In these areas, due to legal or regulatory requirements or stakeholder expectations, the board is an active party in the structures and processes, and in decisions and duties that cannot be delegated to management, which vary by organisation.

The bottom half of the framework depicts areas where the board's responsibility can be described more as active monitor. Here, the board understands the operating models, ascertains that they are adequately developed and resourced, and monitors results of business activities and any issues identified in the process. For many companies, the areas in this category align to planning, operations, compliance, reporting, and risk management.

A governance operating model is the mechanism used by the board and management to translate the elements of the governance framework and policies into practices, procedures, and job responsibilities within the corporate governance infrastructure. In developing the governance operating model, the board balances competing goals (such as the pursuit of growth and the preservation of assets), defines responsibilities (such as those of a business manager and those of a risk manager), and allocates resources to implementing governance. (For more on the Deloitte Governance Framework, see *Framing the future of corporate governance: Deloitte Governance Framework*.⁴)

The remainder of this document presents an enterprise governance operating model that may be suitable for a large FSI company and discusses the characteristics of such a model, elements that might be included, potential benefits, and development and implementation. As an enterprise governance operating model, this model could be adapted to the needs of an entire company or those of specific business units or functional areas.

Components of a governance operating model

A governance operating model defines the mechanisms and interaction points by which governance will be implemented. It enables the board and the executive leadership—as appropriate to their roles and responsibilities—to organise these mechanisms and points of interaction across the organisation’s business lines, legal entities, and jurisdictions. An enterprise-level model, like the one described here, may be adapted to any functional or operating area to promote effective implementation of governance.

As shown in Figure 1, the governance operating model consists of four major components:

- **Structure**, which includes organisation design and reporting structure, committee structures and charters, and control and support function interdependencies
- **Oversight responsibilities**, which define board oversight responsibilities, committee and management responsibilities, accountability matrices, and management hiring and firing authority
- **Talent and culture**, which enable the behaviors and activities required for effective governance by establishing compensation policies (particularly regarding incentives), promotion policies, business and operating principles, performance measurement and management, training, and leadership and talent development programmes
- **Infrastructure**, which comprises governance and risk oversight policies and procedures, reports, measures and metrics, and management capabilities, and the enabling IT and communications support

Within these components, some of the key aspects of an effective governance operating model to be addressed will include:

Board oversight and responsibilities:

The board carries out oversight responsibility across the organisation in areas such as business and risk strategy, organisation, financial soundness, and regulatory compliance. In this regard, the governance operating model should help the board to:

- Articulate the skills and knowledge it requires to effectively execute its oversight responsibilities, and to assess its composition against those needs
- Engage management in providing the information the board requires to exercise governance and risk oversight
- Advise management on policies that ultimately influence the manner in which governance is conducted
- Understand governance activities that occur at various levels within the organisation, and support management in its efforts to enhance programme efficiency, and effectiveness



4 Framing the future of corporate governance: Deloitte Governance Framework, Deloitte, 2012, deloitte.com <http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/IreEng/Page%20Copy/Home/Risk%20Intelligent%20Proxy%20Disclosures%202011_Deloitte_083011.pdf>

Committee authorities and responsibilities:

Effective board committee and management committee structures can help define the number, terms, and qualifications of members, committee responsibilities, reporting and escalation mechanisms, and ways in which board and management committees will interact.

For example, for a management committee, the model could:

- Include committee charters that define the committee's responsibilities and addresses linkages between the committee, the broader executive team, and the board of directors
- Define the types of decisions, investments, events, risks, and other items that should come to the committee's attention (and, when applicable, thresholds or amounts)
- Delineate methods of escalating and reporting significant matters to the appropriate person or committee

Organisational design and reporting structure:

A clear, comprehensive organisational structure normally defines reporting lines for decision-making, risk management, financial and regulatory reporting, public disclosures, and crisis preparedness and response. In an enterprise governance operating model, the organisational structure could enable executive management to:

- Establish the independence and authority of the control functions of compliance, risk, legal, finance, and audit
- Define a process of overseeing the spectrum of risks across all regions and businesses, including strategic, operational, market, credit, liquidity, legal, compliance, property, IT, reputational, and other risks
- Maintain a governance structure that is understandable to internal employees and external stakeholders

Management accountability and authority:

Well-understood authority and accountability for key responsibilities are needed at all levels and in all areas of the organisation. A sound governance operating model could:

- Balance global and regional strategies by delineating the authority and accountability for key roles and specifying a process for resolving or escalating disagreements
- Balance the decision-making authority of business units against that of risk managers, such that risk tolerances and exposure limits are set and observed and risk managers have the authority to challenge those who are taking the risks
- Define clear decision rights such that people understand the authority—and the limits of the authority—associated with their positions
- Provide direction to control functions to assist overseers in determining that businesses are managed within appropriate limits on both global and regional bases

A robust enterprise governance operating model helps enable the execution of governance responsibilities at all levels

Performance management and incentives:

Goals, performance measures, compensation, and incentives should reflect an organisation’s overall commitment to governance as well as principles of asset preservation and risk taking for reward. In this area, the model should help the board to:

- Establish performance objectives that balance asset preservation and risk taking in the pursuit of value creation
- Align incentives to reflect a balance between asset preservation and risk taking
- Specify qualifications and performance evaluations that establish and reinforce the desired corporate culture and tone at the top

A robust enterprise governance operating model helps enable the execution of governance responsibilities at all levels. It does so by clarifying reporting lines and linkages; identifying decisions, risks, and other matters to come to the boards’ or its committees’ attention for review or approval; and promoting an understanding among managers of roles and responsibilities, limits of authority, and means of escalation, and of the balance to be sought between centralisation and decentralisation, autonomy and collaboration, and risk and reward (see sidebar: Striking a balance, repeatedly).

Striking a balance, repeatedly

In practice, governance usually comes down to striking a balance among conflicting needs and goals, which arise in various areas for many reasons.

In general, roles, responsibilities, and decision rights should be conceived and practiced so as to balance the business needs and control/risk-management needs of local operating units and those of the national or regional division and those of the global organisation. This means reconciling two types of needs—business and control/risk-management—along three geographic dimensions: local, national/regional, and global.

For example, in terms of risk governance and management, the goals of value creation through risk taking for reward should be balanced against those of value preservation through risk mitigation and control. Given that risk management is not risk avoidance but management of risks, it is useful to consider the three traditional lines of defense—business management, risk management, and internal audit—and how the governance model can define their respective roles and responsibilities.

As in any situation of competing forces, balance is dynamic. In an organization, they should have mechanisms to guide their decisions, interactions, and upward and downward communications. An effective governance operating model has the potential to provide those mechanisms.

The power and benefits of a governance operating model

The power of a governance operating model can lie in its specificity. The required or desired level of specificity in the operating model will vary from organisation to organisation. This is appropriate. Governance frameworks define principles and, usually, responsibilities. But they largely leave individual organisations to define how governance roles will be assigned, how roles will interact, and how responsibilities will be fulfilled.

FSI companies may benefit from an effective governance operating model in the following ways:

- **Improved clarity:** The board and management face the challenge of translating governance principles into practices. The governance operating model could provide a vehicle for the board and its committees to address this challenge by clearly defining the roles, responsibilities, accountabilities, information flows, and guidelines that people need in order to implement governance
- **Greater visibility:** To fulfill its governance responsibilities, the board should have clear lines of sight into management's decision-making and risk-management processes. In the governance operating model, the board could establish those lines of sight, for example, by stating the types and amounts of investments and transactions and the risk exposures that should come to its attention

- **Improved coordination:** Addressing the complexity inherent in governance of multiple businesses across a global organisation requires coordinated action. It also entails balancing considerations regarding centralisation versus decentralisation and considering local business, customer, compliance, legal, and other stakeholder needs—which the model should be able to address
- **Increased effectiveness:** A model that specifies the information that the board and its committees require—and from whom, how often, and under what circumstances they will receive that information—may assist the board in executing governance more effectively

The model should arrange the governance and risk oversight process—and the related infrastructure and IT support—such that responsibilities are carried out in a reliable manner. The overarching benefit of a sound governance operating model is that it could enable the board and its committees to execute their responsibilities properly and with greater assurance that they have done so.



Designing the governance operating model

Each component of a governance operating model consists of subcomponents comprised of activities, only a sampling of which are listed in Exhibit 3 by way of illustration. A governance operating model can provide substantial detail regarding the ways in which

activities will be conducted to implement governance. Indeed, one of the main reasons to create a governance operating model is to define and document the processes, procedures, and reporting mechanisms that will constitute governance, along with the training, IT, and other resources that will be needed.

Figure 3: Illustrative activities in designing the governance operating model

Components	Subcomponents	Description
Structure	<ul style="list-style-type: none"> • Committee structure and charters • Organisational structure and reporting lines • Control and support functions' roles 	<ul style="list-style-type: none"> • Outlines board and management committee structures, mandates, membership, and charters • Establishes design of governance framework • Delineates organisational structure, reporting lines, and relationships • Highlights role and independence of control and support functions from business owners
Oversight responsibilities	<ul style="list-style-type: none"> • Committees authorities and responsibilities • Management accountability and authority • Board oversight and responsibilities • Reporting, escalation, and veto rights 	<ul style="list-style-type: none"> • Outlines the type of committees (board and management) and associated responsibilities • Specifies functional accountabilities for day-to-day management of business practices across the enterprise • Delineates board and management approved policies supporting delegation of authority (decision rights) including reporting, escalation, and veto rights
Talent & culture	<ul style="list-style-type: none"> • Business and operating principles • Core beliefs and risk culture • Leadership development and talent programmes performance • Management and incentives 	<ul style="list-style-type: none"> • Aligns governance with operating and business principles • Articulates core beliefs and foundation for culture • Highlights characteristics of risk culture • Outlines leadership succession, assessment, and development responsibilities • Aligns performance management, approach, measures and responsibilities to compensation and incentive plans
Infrastructure	<ul style="list-style-type: none"> • Policies and procedures • Reporting and communication • Technology 	<ul style="list-style-type: none"> • Establishes design and content of policy manuals and associated procedures • Outlines type and frequency of internal reporting and communications • Defines scorecards, measures, and metrics to track performance • Aligns technology and governance requirements

Copyright © 2013 Deloitte Development LLC. All rights reserved.

Developing the governance operating model entails defining and documenting the subcomponents and activities at the level of detail the organisation requires to inform peoples' decisions and actions. The goal is not to dictate, but to define decisions and actions in ways that will be meaningful from a governance standpoint. The process of documenting the governance operating model can create as much value as the resulting documents.

If an organisation has an undocumented governance model, documenting it may focus decision makers on balancing competing objectives, defining responsibilities, allocating resources, and devising solutions—activities essential to implementing governance.

In defining its governance operating model, the organisation may assess its current state, define its desired future state, and identify the steps required to achieve the latter, that is, to effect implementation. In this exercise, the organisation should consider addressing the following considerations and objectives:

• **Compliance issues:**

- Achieve compliance with multiple, sometimes conflicting, requirements
- Reconcile business requirements with regional and/or parent-company country regulations
- Align regulatory compliance and risk management to address needs in an integrated, globally coordinated manner

• **Cultural shift:**

- Move toward one corporate culture across the organisation
- Resolve the tension between local customs, regulations, and business-unit needs and the desire to set the tone from the top
- Resolve the tension between centralisation of risk policies and decentralisation of business decision making

• **Governance and management decision rights:**

- Establish ownership for decisions for strategy, budgets, funding, liquidity plans, recruitment, performance management, compensation, risk management, and new business and product approvals
- Clarify board oversight roles and responsibilities and their relationship to management roles and responsibilities
- Define who takes the lead, who has consultation/veto rights, and how conflicts and disagreements are to be resolved

• **Process and system issues:**

- Enhance processes and systems for business-line managerial and risk reporting to support regional and divisional risk management
- Upgrade processes and systems to generate data and reports required by local regulators
- Rationalise and harmonise controls to enhance performance and reduce costs

• **Regulatory relations:**

- Designate an on-site point person to respond to local regulators' questions when required or useful (rather than routing them to headquarters)
- Establish virtual (or actual) holding companies at the local level with key executives who can respond to regulators' requests regarding multiple local business units
- Address regulatory requirements regarding subsidiaries, affiliates, and alliance partners

• **Human resources:**

- Identify job specifications and roles required in a matrix reporting structure, and the required skills, experience, and expertise
- Account for skills, experience, and expertise required at the board level, particularly in areas of governance and risk oversight

When crafting governance and exercising oversight, boards and executive teams may do well to bear in mind the goal of creating a risk intelligent culture (see sidebar on page 36: A Risk Intelligent Culture).

A Risk Intelligent Culture

While policies, procedures, and rules are useful and necessary, the organisation's risk culture largely determines how it manages risk and the attention paid to guidelines.

The following are characteristics of a risk intelligent culture:

- **Commonality of purpose, values, and ethics:**
People's individual interests, values, and ethics are aligned with those of the organisation's risk strategy, appetite, tolerance, and approach
- **Universal adoption and application:**
Risk is considered in all activities, from strategic planning to day-to-day operations, in every part of the organisation
- **A learning organisation:**
The collective ability of the organization to manage risk more effectively is continuously improving
- **Timely, transparent, and honest communications:**
People are comfortable talking openly and honestly about risk using a common risk vocabulary that promotes shared understanding
- **Understanding of the value of effective risk management:**
People understand, and enthusiastically articulate, the value that effective risk management brings to the organisation
- **Responsibility—individual and collective:**
People take personal responsibility for the management of risk and proactively seek to involve others when that is the better approach
- **Expectation of challenge:**
People are comfortable challenging others, including authority figures. The people who are being challenged respond positively

The board is responsible for advising management on the risk culture and for overseeing management's efforts to maintain an appropriate risk culture.

One of the main reasons to create a governance operating model is to define and document the processes, procedures, and reporting mechanisms that will constitute governance, along with the training, IT, and other resources that will be needed

Enhancing or establishing a governance operating model

The following is a suggested three-part approach to enhancing or establishing a governance operating model. While it is not practical for the board to perform the tasks in each of these steps, nor within its purview, the board is usually positioned to commission these tasks to be carried out within the organization or by external specialists.

Part 1. Define the governance operating model requirements

- Identify potentially useful governance frameworks
- Identify applicable regulatory and governance requirements
- Consider governance scope and needs, such as domestic, global, business line, and those involving existing and contemplated products and processes
- Define the current state of governance, as well as gaps and considerations

Useful steps within Part 1:

- Analyse peers at a summary level (for example, by means of their committee charters, which are often publicly available)
- Assess the organisation's governance vis-à-vis a governance maturity model
- Identify and prioritise governance needs and activities

Part 2. Design the governance operating model

- Define the desired future-state for the headquarters region, global business operations, and control functions, such as risk, legal, compliance, finance, audit, and HR (see Figure 3 for illustrative activities in designing the governance operating components and sub-components.)
- Define a change-management plan to institutionalise the attitudinal and behavioural changes needed to implement the model

Useful steps within Part 2:

- Detail design of governance operating model and its components
- Develop matrix defining key accountabilities across the organisation
- Develop matrix defining decision rights and escalation paths

Part 3. Implementing the governance operating model

- Create an implementation plan that:
 - Defines standards and metrics by which success will be measured
 - Maps governance requirements to organisational functions and business requirements
 - Allocates resources to implementation, per priorities and over time as requirements and resources permit
 - Defines schedule and components of review process
- Implement the plan and maintain governance practices
- Evaluate the plan, implementation, and practices

Useful steps in Part 3:

- Create an implementation plan in an electronic, visual format that enables the team to track progress on action steps and to log disposition of risks and related issues
- Obtain external assistance in creating a workable plan and format and in overseeing implementation, as necessary

Defining governance operating model requirements, designing the governance operating model, and planning and carrying out implementation are significant undertakings for any financial organisation. In addition, it may be an iterative process, with aspects of the model subject to change or adjustment during or after implementation, and in response to changing regulatory or business conditions. However, the process outlined here represents one route toward enhancing governance at FSI companies, and one that can be rationalised, planned, resourced, monitored, and evaluated.

Getting governance done

In some FSI companies, the need for a clearly documented governance operating model has become acute. This is understandable. Board responsibilities have increased due to the need to continue to oversee management of growing, complex, global institutions amid challenging business conditions and rising stakeholder expectations. The board and its committees now have more to oversee, and management and its committees have more regulatory and governance considerations to address—as well as more risk to manage.

Although boards at FSI companies may have adopted governance frameworks and strengthened their risk governance, work remains to be done if the many governance needs of large, complex institutions are to be met. A well-documented governance operating model may assist the board and its committees in meeting these needs.

The desired governance operating model—meaning the right model for the organisation—assists the board to get governance done. The right model should promote clarity and understanding of the ways in which people in governance roles and in management roles execute their responsibilities. It can do so by assisting the board and management to specify ways of implementing governance. Despite significant recent progress in the area of governance, this is an apparent urgent need at many, global financial services companies.





Aligning risk and the pursuit of shareholder value

Risk transformation in financial institutions

Scott Baret
Partner
Deloitte US
Global Enterprise Risk Services Leader
Financial Services
Deloitte Touche Tohmatsu Limited

Laurent Berliner
Partner
Deloitte Luxembourg
EMEA Enterprise Risk Services Leader
Financial Services

Julian Leake
Partner
Consulting
Deloitte UK

Peter Matruglio
Partner
Enterprise Risk Services
Deloitte Australia

Leon Bloom
Partner
Enterprise Risk Services
Financial Services
Deloitte Canada

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 Touche Tohmatsu Limited (DTTL) published in 2013 *'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.

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 deemphasise 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.

2. Extensive industry and regulatory requirements

Global financial institutions with multiple lines of business must respond to myriad 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.

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 help improve data quality, accessibility and analysis, setting the scene for improved risk management and business management.

Impact on drivers of shareholder value

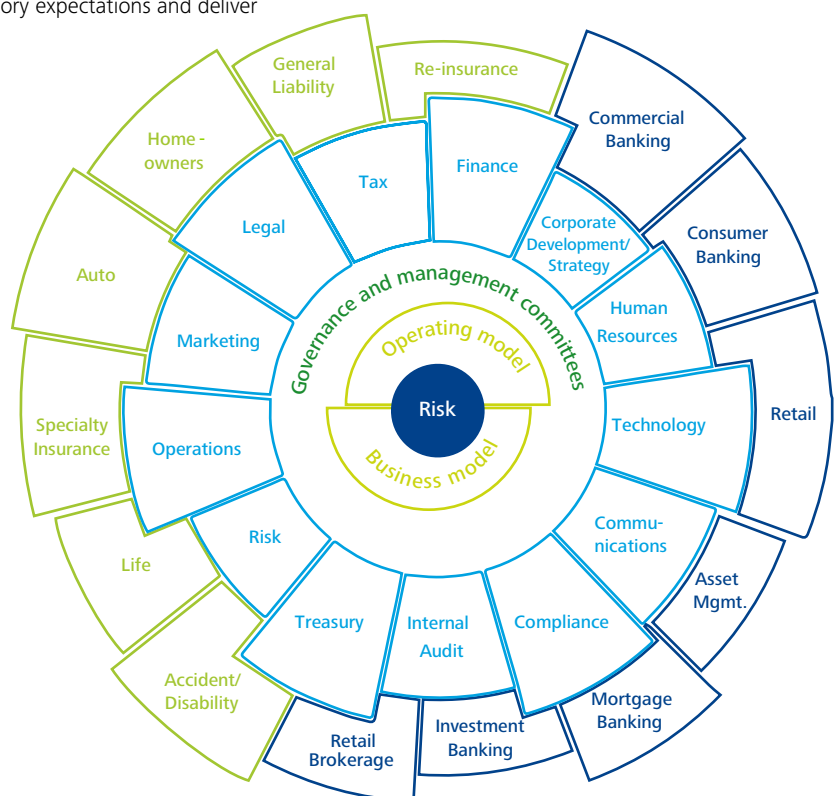
Shareholder value is driven principally by achieving a positive spread between the risk-adjusted return on capital and the cost of capital, and factors such as operating costs and taxes. These drivers are impacted by specific forces and market conditions affecting the business. A focus on shareholder 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



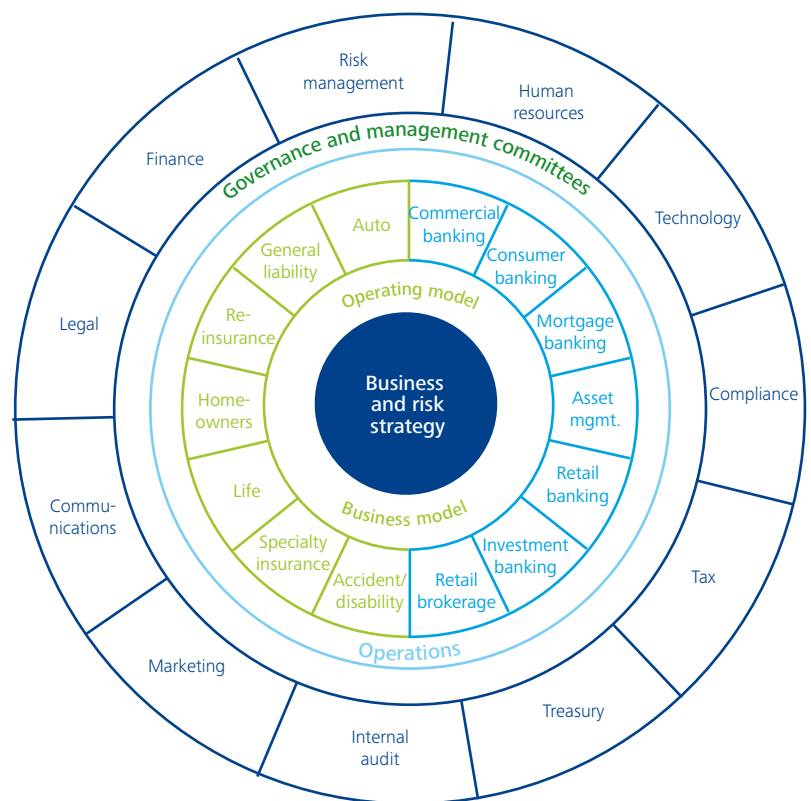
Misalignment and gaps develop over time, sometimes over decades, as an organisation diversifies its businesses, introduces new products and services, and responds to new laws and regulations. Some business units come to see the risk management function as being responsible for managing risk, whereas 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.

Figure 2: Alignment in a financial institution

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



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. These choices are often 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 (listed below)—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 risk management function then supports each business in operating within the risk profile each requires in order to meet return objectives

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.

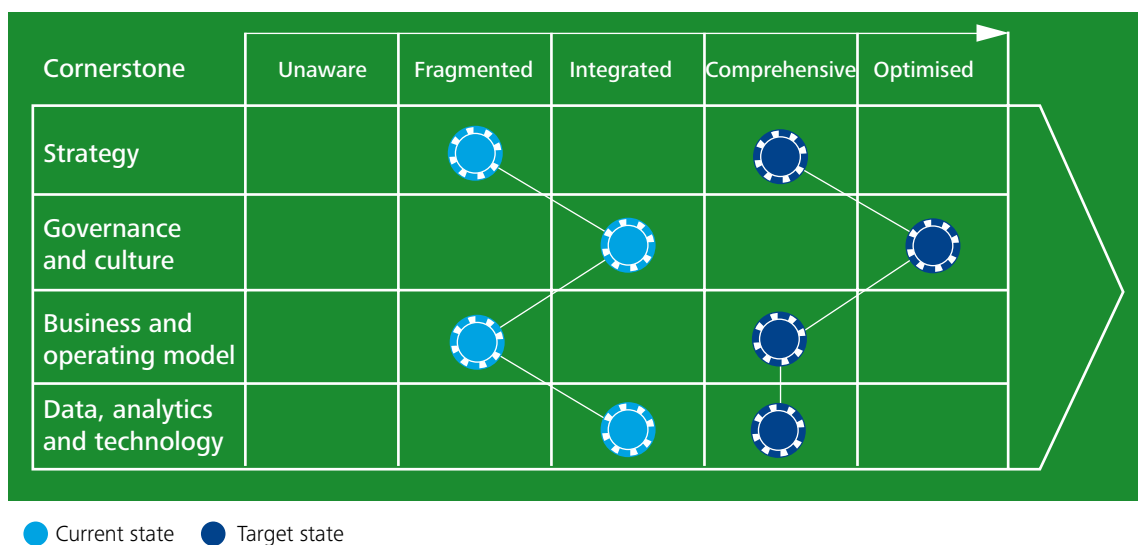


Assessing needs

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. 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:

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'

- **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 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.

Reprinted with the permission of Deloitte Touche Tohmatsu Limited.



Funds Transfer Pricing

A gateway to enhanced business performance

Jean-Philippe Peters
Partner
Governance, Risk
& Compliance
Deloitte Luxembourg

Arnaud Duchesne
Senior Manager
Governance, Risk
& Compliance
Deloitte Luxembourg

Olga Slabari
Consultant
Governance, Risk
& Compliance
Deloitte Luxembourg

Funds Transfer Pricing (FTP) is both a regulatory requirement and an important tool for managing a firm's balance sheet structure and measuring risk-adjusted profitability, taking into account liquidity risk, maturity transformation and interest rate risk. It enables costs to be transferred from central treasury functions to the products and business lines originating these costs and the related risks.



While FTP systems have been designed and in place at many financial institutions for a while, the increased scrutiny of supervisory bodies regarding risk, liquidity and performance management in banks that followed the 2007-2008 financial turmoil have shed further light on these mechanisms and their weaknesses.

To address identified loopholes and ensure the implementation of appropriate risk transfer mechanisms, the European authorities issued a set of guidelines¹ that was later transposed into local circulars (e.g. CSSF Circular 12/552, as amended, in Luxembourg). The notion of risk transfer pricing emerged in this context, and goes beyond the traditional FTP concept, which used to be largely focused on transferring the liquidity cost and ALM risks

to fund users. Risk transfer pricing is a mechanism that, in its most mature state, is established to price all risks to which the various departments of the organisation are exposed, influencing the volumes and terms upon which business lines trade in the market, and promotes more resilient, sustainable business models. In this article and for the sake of simplicity, we will refer to the notion of FTP² as a general mechanism established to price all the risk taken on by a financial institution.

In this article, we review the fundamental principles encompassing an FTP mechanism, the various forms it can take, and how it interacts with recent regulatory changes.

¹ In 2010, the CEBS issued Guidelines on Liquidity Cost Benefit Allocation

² The move from FTP to risk transfer pricing is done through the inclusion of a risk premium that relates to a number of risk parameters, e.g. client creditworthiness, the nature of the business (leverage buyout, mortgage loan, consumer loan, etc.), the nature of the operations, etc.

The origin of the Funds Transfer Pricing

Over the past 40 years, the organisational structure of large financial institutions and the way they are managed has evolved from a geographic organisation (branch manager in charge of a single, undifferentiated line of business) to a business line structure (creation of distinct and 'autonomous' business lines across geographical areas). This organisational transformation created the need for new management tools to overcome the two main issues that materialised with this change (risk management and performance management).

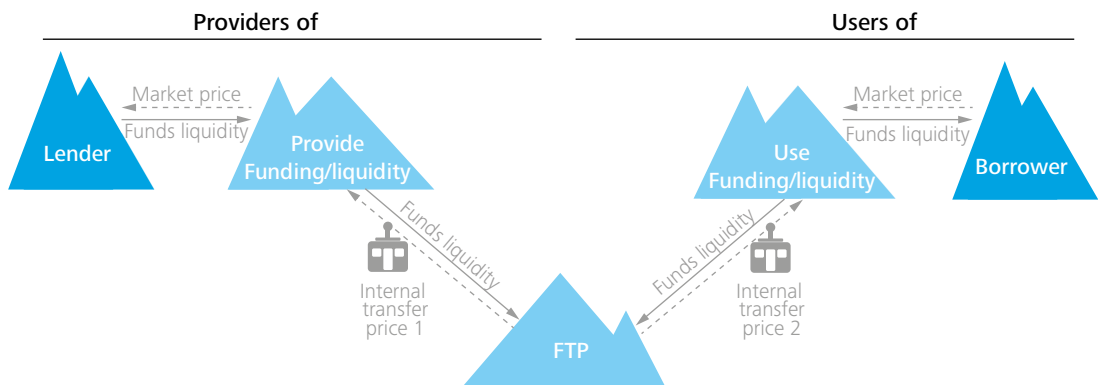
The way financial institutions manage and assess risk and performance internally is closely intertwined with choices made in terms of operational structures. Banks organised according to the geographical principle consist of separate subsidiaries in charge of both the origination and placement of funds. Their risks and performance are therefore determined locally, and are

heavily influenced by the local financial environment. From another perspective, financial institutions organised around supra-geographical business lines have to assess their risks and returns, taking into consideration, on the one hand, the activity of the business lines, and remuneration for the centrally-raised funds on the other. This structural transformation thus created the need for a transfer price mechanism between the entities, allowing for risk and performance management at individual level.

From a management accounting concept to strategic management tool

Over time, the FTP systems implemented by financial institutions have gained in complexity as the industry started to produce more detailed revenue breakdowns, to understand where and how they were making money, as well as the potential risks involved. This section illustrates this trend and introduces some widespread approaches developed in the industry.

Figure 1:



As a result, most banks began to develop and implement FTP systems. Conceptually, funds-generating businesses were seen as originators of funds to be sold in an internal capital market to fund-using businesses.

With the implementation of such system, a transfer rate is used to divide the bank's overall Net Interest Margin into two sub-margins (one for asset origination and the other one for liability origination) corresponding to the economic value obtained from each activity taken separately.

- **Single rate FTP systems**

Most banks started their FTP journey using a single transfer rate representing a weighted blend of external market prices for the available funds. With this simple approach, the FTP mechanism failed to take into account the existence of a sloped yield curve, potentially incentivising the development of sub-optimal deals from a bank-wide viewpoint. Assuming a positive slope yield curve, the single-rate FTP mechanism could encourage the bank to enter into longer maturity loans to maximise the spread between the interest rate applied to these loans and the single transfer rate. Conversely, the funding business unit could be encouraged to collect short-term deposits to increase the spread between the actual cost of funds and the single transfer rate. Overall, this means that the bank ends up with a large maturity mismatch that needs to be handled centrally to reduce the liquidity risk created by the FTP mechanism³.

As the use of a single transfer price does not account for maturity mismatches between sources and uses of funds, it is easy to see that this approach would only be effective in a situation of relatively homogenous products across business units, and would fail to satisfy the needs of more complex financial organisations.

- **Multi-rate, Matched Maturity FTP systems**

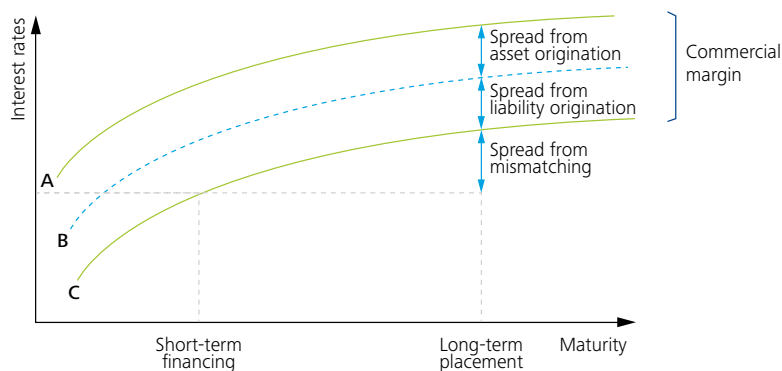
Multi-rate, matched maturity FTP systems represent a clear improvement on single-rate pricing systems, as they are based on a more comprehensive approach, creating multiple pools of funds with different characteristics (e.g. maturity, credit risk, etc.) matching the characteristics of the invested funds or even of individual transactions. In these systems, a business generating six-month certificates of deposit would be assigned a six-month transfer rate existing at the moment of the origination, and would carry this rate until maturity.

The same principle is applied to the asset origination business, with the FTP mechanism providing an incentive to manage assets and liabilities irrespective of their maturity, insulating individual business units from most interest rate risks, as these are transferred to the central treasury function⁴ administering the FTP system.

The matching of funding and lending characteristics can be used by organisations to not only allocate funding costs, but to identify risk exposures arising from mismatches in their characteristics as well. For instance, by matching liability maturities (i.e. sources of funds) with asset maturities (i.e. use of funds), the funding centre will accumulate the information on mismatches at pool level, which it will then be able to hedge on an aggregated basis. This possibility to obtain information and manage maturity mismatches makes FTP systems valuable tools for asset-liability management. Moreover, these mechanisms mean that individual business lines can operate on a fully hedged basis and concentrate on their key source(s) of risk(s), e.g. credit risk for the asset origination business. This structural approach involves a disaggregation of the net interest rate margin into three internal spreads corresponding to the specific risk dimension supported by each entity.

Multi-rate, matched maturity FTP systems may be based on different levels of complexity, with the more advanced models using multiple marginal cost of funds curves to improve the pricing accuracy of placed funds.

Figure 2:



3 Automatically updating the single transfer rate would never be enough to mitigate the conceptual weakness inherent in the single-rate FTP mechanism. A single transfer rate might encourage the collection of short-term liabilities, thus increasing the bank's refinancing needs

4 The treasury function is viewed as a central department responsible for the management of asset and liability issues, with the aim of supporting the bank's commercial development



- **FTP and prepayment risk**

In its classic form, a multiple-rate, matched-maturity FTP system does not insulate business units from prepayment risk. As most loans can be prepaid by the borrower at will, this could adversely affect some operations under the classic multiple-rate, matched-maturity FTP system. In the event of early redemption, the assets side of the business is affected while the related liability will remain at the initial cost. Even if the bank invests in a new asset with the same maturity as the redeemed loan, it will not deliver the same remuneration, since the new asset will carry the interest rate associated with the residual maturity. Moreover, the impact for the business unit will get worse in case interest rates fall since the inception of the initial loan.

To overcome this situation, banks have started to price the embedded call option attached to the loan issued by the business unit. With the integration of such characteristics within the FTP system, the bank's treasury encourages the business unit to charge the customer an appropriate premium for the prepayment risk borne by the bank. Moreover, the treasury function is able to handle this risk at an aggregated level.

Today, well-defined FTP systems go beyond the single or multi-rate funding structures. The approach enables the integration of different risk components to the notional interest rate curve. Such components may include characteristics of the financial institution, such as credit spread, bank-wide currency adjustments, contingent liquidity add-ons and the potential impact of any other financial risks, while at the same time reflecting characteristics of specific transactions such as maturity, embedded options and contingent liquidity costs.

Adjusting transfer price systems to organisational complexity and the economic environment

As discussed in the previous section, the performance of an FTP system in addressing the goals of the organisation is directly dependent on its design and ability to take into account the relevant specific features and complexity of the organisation and its products. The desired degree of complexity in establishing FTP systems may be achieved through making choices on the main elements of its design.

- Model granularity:**
 transfer prices may reflect the characteristics and riskiness at the bank-wide level or be more granular to capture the specific risk of products
- Current rates versus historical rates**
 simple transfer pricing methodologies rely solely on prevailing interest rates, whereas more comprehensive approaches may leverage on the historical rates applicable at the time the investment was made
- Incorporation of the economic cost of specific product features:**
 depending on the maturity of the transfer pricing system, it may (or may not) incorporate features of liquidity placements, such as caps, conversion or prepayment options
- Marginal cost of funds:**
 systems may adjust the interest rate curve to the credit capacity of the bank, reflecting its marginal cost of funds, or they may use a single interest rate irrespective of the volume of funds used by the departments

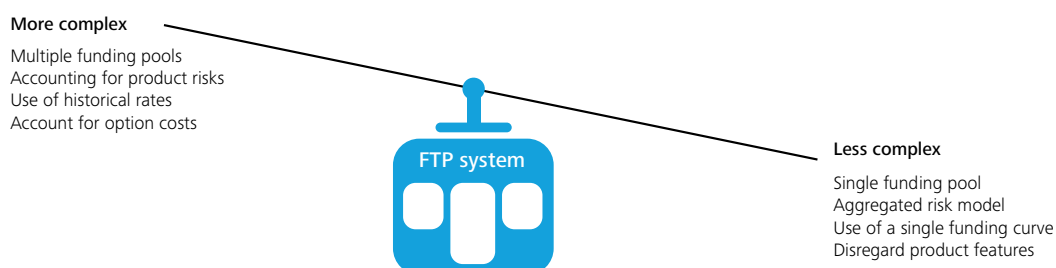
To illustrate the link between the complexity of FTP methodology and its impact on the organisation, we consider the case of a single funding pool. In this context, the lending departments will favour longer-term placements, as they will increase the profitability of their activities when compared to the single average cost of funds, and this will have a direct impact on the composition of the lending portfolio.

The features of other products, such as embedded options, may make them more appealing to lending departments, unless they are more expensive to fund through transfer prices. Not reflecting features such as maturity, options or prepayment risk in transfer prices may thus have a direct impact on the profitability of the organisation, as in this case the funding centre will ultimately carry the cost of the related risks without additional compensation.

It therefore follows that for an FTP system to be successful in fulfilling all its objectives, including the implementation of strategic decisions within the organisation and the safeguarding of its financial stability, it has to reflect the complexity of the organisation and potential changes to its environment. As is often the case with models and methodologies, it is up to organisations to find the right balance between the complexity of the model and the added accuracy.

It is easy to see that the decisions made in establishing transfer prices have a direct impact on the activity of the organisation.

Figure 3:



Through their impact on the definition of the risk-adjusted performance of the various departments, FTP systems are a valuable tool for strategic decision-making. The FTP mechanism can identify the most profitable activities on a risk-adjusted basis and the incentivising activities aligned with the strategic direction of the institution.

Consistent design and application of transfer prices may be used by the management to:

- Influence the overall business mix by identifying (un)profitable departments from risk-adjusted point of view
- Influence the product mix by adding different transfer price spreads, depending on the desirability of the products
- Influence pricing and transaction volume decisions to bring them in line with the organisation’s goals
- Create relevant performance benchmarks by selecting appropriate underlying curves

Linking FTP with regulatory requirements

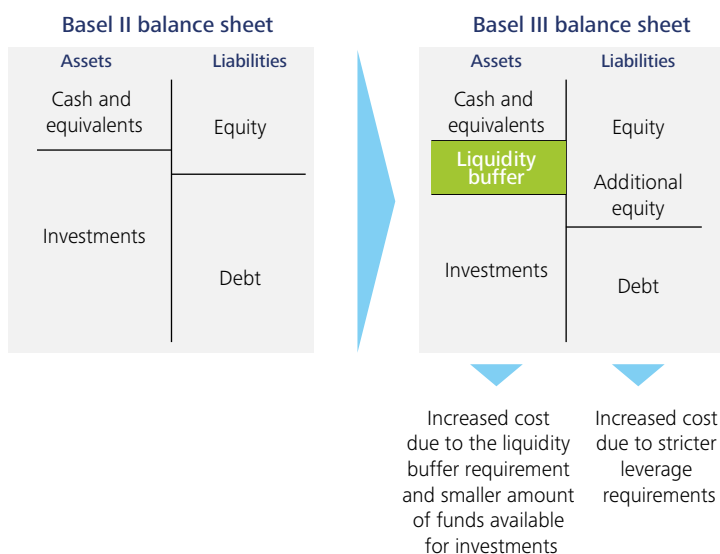
In response to emergence of regulatory requirements such as Basel III/CRD IV, the FTP concept has received increased attention. As financial institutions face pressure to hold more capital to cover their risks, and to hold more liquidity to guard against potential market disruptions, the need to embed regulatory and risk management considerations in the strategic decision-making process of the organisation becomes even more important.

The liquidity requirements introduced by Basel III/CRD IV can be seen as an opportunity cost for financial institutions, forcing them to hold a cushion of very high quality liquidity at the expense of higher yield-generating assets.

On the flipside, this cushion provides resilience against potential internal and external liquidity shocks, when the bank may be unable to fund its activities through its normal funding sources. Holding additional liquidity may therefore be regarded as providing an economic benefit to the organisation, reducing its overall riskiness and facilitating cheaper funding.

The interactions between these factors have to be fully understood and embedded in the FTP mechanism. In this context, FTP comes as a natural tool for achieving those goals, facilitating the allocation of costs and benefits across business lines, and ensuring that these requirements are embedded in all business decisions.

Figure 4:



We can illustrate this concept using a simple example. Consider a lending department that issues a committed credit line to a customer. Given the Liquidity Coverage Ratio (LCR) requirement, this exposure would have to be covered by high-quality liquid assets. As such, assets might have a negative impact on the bank's profitability, the foregone profit may be embedded in the transfer price of funds via a liquidity mark-up reflecting the specific product features.

At the same time, as the bank would now hold a higher amount of high-quality assets, the base interest rate charged may decrease somewhat, reducing the transfer price. By combining those two impacts and by providing the lending department with a transparent transfer price, the bank could facilitate informed decision-making processes that contribute to the best interests of the organisation as a whole.

Following a similar mechanism, banks may also include additional components affecting regulatory capital requirements in transfer prices, for example, compensation for higher credit risk caused by the specific exposures or even specific operational risks associated with a product, activity or client type.

Through its impact on the allocation of profit margins between the bank's departments, the transfer pricing mechanism is a sensitive topic, as it used to evaluate the performance of business units, and given that it has a direct influence on the bank's risk profile. In the aftermath of the financial crisis, regulators turned their attention to the governance of FTP systems, requiring financial institutions to ensure that they create

Well-developed FTP systems may serve as a valuable strategic management tool, supporting commercial development through an appropriate FTP set-up

incentives aligned with the principle of sound and prudent business management. For instance, recent regulations require the establishment of transparent and consistent transfer pricing mechanisms that include the impact of liquidity costs, as well as robust approval and supervision procedures.

In Luxembourg, the CSSF has enlarged the scope of its requirements to cover the establishment of FTP practices pertaining to liquidity, ALM risk, and other types of risk (e.g. credit risk, FX risk, operational risk, etc).

In this context, the governance of FTP systems becomes a highly important component of their design, not only in relation to regulatory compliance, but also to ensure sound management and strategic alignment within the organisation.

Conclusion

FTP has gained importance in modern banks, given the multiple roles it fulfils in terms of product pricing, liquidity management, performance measurement, balance sheet steering and regulatory compliance. FTP frameworks should be commensurate with the bank's activities and size, varying in complexity and methodology, and processes accordingly.

Located at the heart of the relationship between different bank units, the FTP framework should be fully integrated within a bank's overall organisational model. If it captures the specific characteristics of the organisation effectively and is properly aligned with the ever-evolving supervisory expectations, the FTP mechanism can prove to be a valuable strategic management tool for senior managers of financial institutions.



Small and Medium Enterprises in a globalised, post-crisis world

Reacting to new treasury risks and challenges with cash pooling solutions

Petra Hazenberg
Partner
Strategy, Regulatory
& Corporate Finance
Deloitte Luxembourg

Edouard Hansoulle
Senior Consultant
Strategy, Regulatory
& Corporate Finance
Deloitte Luxembourg

Esther Bauer
Analyst
Strategy, Regulatory
& Corporate Finance
Deloitte Luxembourg



Different cash pooling solutions and tools have been available to companies for some time now. However, as companies act in a changing, increasingly globalised environment, the strategic importance of cash pooling becomes ever more important in facing daily challenges.

While mature Multinational Corporations (MNCs) mostly already have professional cash management solutions, many Small and Medium-sized Enterprises (SMEs) are less well equipped.

Facing market, financing and operational risks through entering international markets, SMEs require more professionalised cash management solutions, such as cash pooling. These can assist them in limiting their exposure to market, financing and operational risks. However not all cash pooling tools are equivalent and in order to limit exposure to risk optimally, SMEs will need to choose cash pooling solutions carefully. Banks will need to offer solutions that can be adapted to the needs and particularities of SMEs, which are flexible and integrated.

The question that arises is:

'Are today's financial institutions sufficiently equipped to provide these solutions to SMEs?'

Introduction

Often overlooked regarding their importance to the global and European economy, SMEs represent 99% of all businesses in the European Union and are responsible for 65% of employment and €3,666 trillion¹ in value added. As they are reacting to a changing environment, SMEs are increasingly becoming international and their contribution to the economy is likely to remain high. Increasingly international and in a post-crisis world, SMEs need new cash management solutions that can help them manage new market, financing, liquidity and operational risks.

¹ European Commission, Annual Report on European SMEs 2013/2014

A changing environment for SMEs

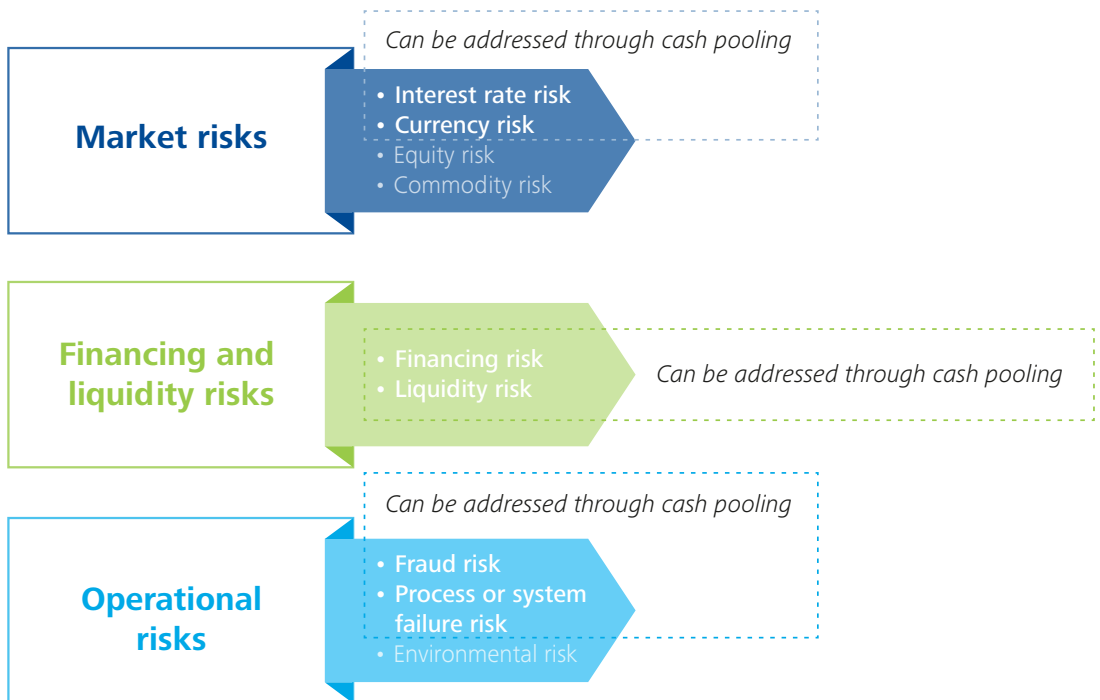
As globalisation is becoming an increasingly important reality, with more competition from abroad, but also an immense array of opportunities for new markets, SMEs are progressively jumping on the band wagon and becoming international. A survey carried out by the European Commission in 2009 showed that 42% of European SMEs are currently involved in international business activities and 25% of European SMEs are exporting products to foreign markets².

With the World Trade Organisation (WTO) forecasting international trade flows to rise by 3.5% in 2014 and 4.0% in 2015³, the development towards increasing internationalisation of SMEs is likely to continue with more and more SMEs having more and more complex structures to manage.

Focus on cash pooling

- What is cash pooling?
Cash pooling is a cash management technique used by companies to consolidate their credit and debit positions across multiple accounts. Different cash pooling solutions exist, notably physical and notional cash pooling
- What is the difference between physical and notional cash pooling?
The main difference between physical and notional cash pooling is that with notional pooling, there is no physical transfer of funds between accounts to balance, while physical pooling involves a physical transfer of cash between accounts

Figure 1: Cash Pooling can help SMEs in addressing some of the treasury risks they face



² European Commission, Annual Report on European SMEs 2013/2014

³ www.wto.org/english/news_e/pres14_e/pr722_e.html

As a result of adapting to the changing environment, SMEs will increasingly be exposed to market risks and will need to adapt their cash management strategies

Traditionally working tightly with one or a limited number of house banks in domestic markets, the shift towards internationalisation is increasingly pushing SMEs into a more complex multi-bank, multi-currency environment. SMEs need to adapt their treasury and cash management strategies when adapting to the changing environment. Through internationalisation, SMEs will typically increase the number of subsidiaries, as well as the number of cross-border activities leading to a higher exposure to market risks.

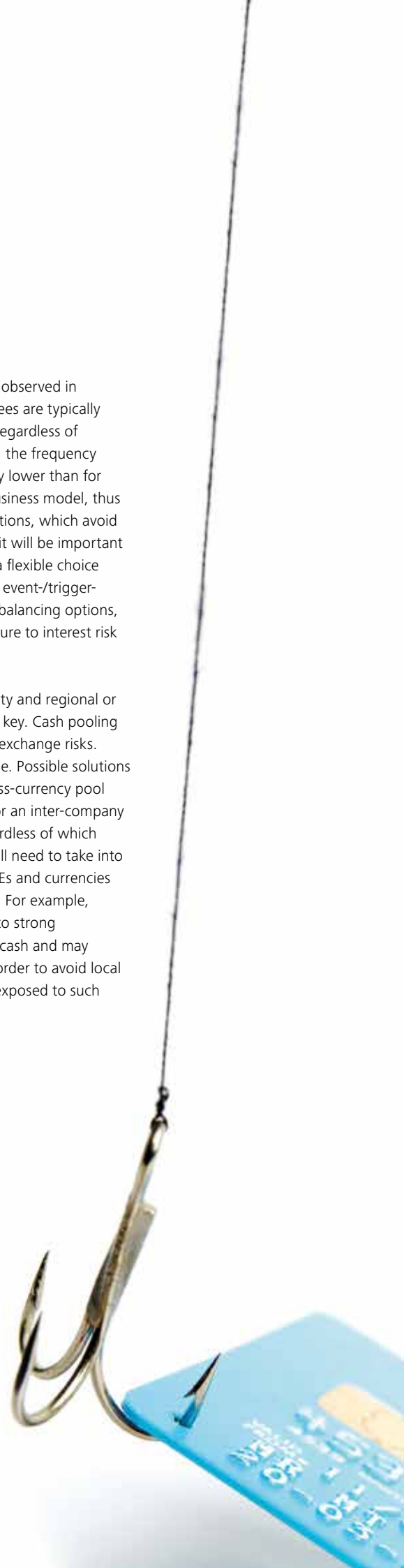
Market risks, to which SMEs are mainly exposed, are interest rate risks and currency risks. Developing international subsidiaries will require SMEs to set up additional bank accounts in the countries they are entering. As the number of bank accounts that an SME possesses increases, the probability of excess or insufficiency of cash balances on the different accounts increases. This results in a significant exposure to losses due to interest rate fluctuations, which intensifies with the amount of excess or insufficient held.

As cross-border activities increase, it is also likely that the number of currencies in which a company is active will increase. As this happens the transaction-related risk (the risk that the cash flows and profits of the company will be impacted by movements in foreign exchange markets) will increase. This risk is heightened by geopolitical developments in international markets and attractive emerging markets in particular.

Cash pooling tools can assist SMEs in this context, as balancing activities will consolidate cash positions, reducing excess, idle cash as well as debit positions on the different accounts and reducing interest risk. However, SMEs have specificities that are different to MNCs and tools offered for SMEs must take these differences into account.

For instance, current pricing models observed in the industry show that transaction fees are typically charged per sweeping transaction, regardless of the amount of the sweep. For SMEs, the frequency and regularity of transfers are usually lower than for MNCs, and depend highly on the business model, thus requiring banks to offer flexible solutions, which avoid unnecessary transfers. In particular, it will be important for banks to offer tools that permit a flexible choice of frequency of sweeping (including event-/trigger-based sweeping), as well as flexible balancing options, allowing SMEs to reduce their exposure to interest risk without charging unnecessary fees.

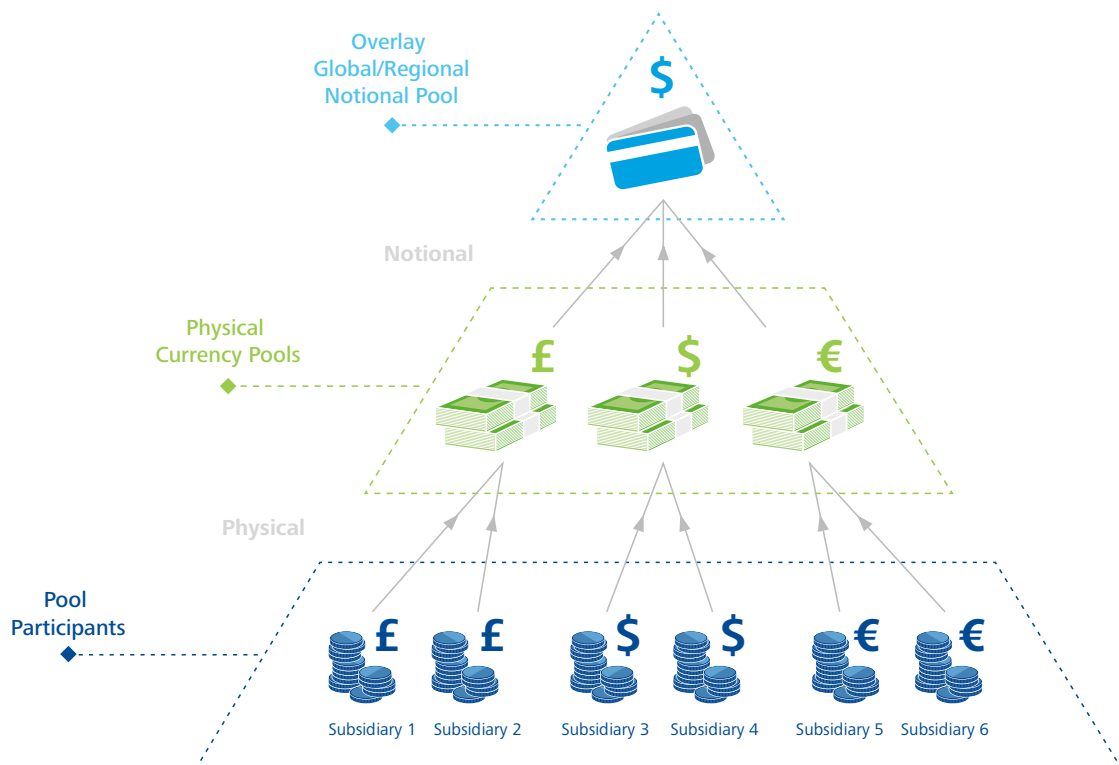
In dealing with currency risk, flexibility and regional or global integration of the tool will be key. Cash pooling will allow an SME to reduce foreign exchange risks. Different possibilities exist in this case. Possible solutions include the overlay of a notional cross-currency pool over single currency physical pools or an inter-company loan-based physical cash pool. Regardless of which option is chosen, however, banks will need to take into account that business models of SMEs and currencies in which they are active vary greatly. For example, while certain SMEs will be exposed to strong geographic seasonal fluctuations of cash and may therefore prefer physical sweeps in order to avoid local cash shortages, others may be less exposed to such fluctuations.



Flexibility regarding currencies offered in the pool or the master account as well as proposing different solutions is therefore essential in supporting SMEs to reduce foreign exchange risk. To support SMEs in their risk

assessment process, tools need to offer an integrated view of the different cash positions across currencies. Providing such an integrated view will assist the central treasury in identifying and assessing currency risks.

Figure 2: Single currency physical pools with a notional overlay pool allow the reduction of currency risks



Financing risk and liquidity risk have become more significant for SMEs following the crisis and efficient cash management can help reduce these risks

While globalisation has significantly affected SMEs in Europe and around the world, the financial and economic crisis is also a non-negligible factor. During the financial crisis, SMEs appeared to be less vulnerable to the effects of the financial crisis than larger MNCs⁴. However, in the post-crisis era, the environment has become more and more difficult for SMEs, who are finding access to short and long-term funding difficult. As the annual report on European SMEs 2013/2014 demonstrated, access to finance is the second most important issue for SMEs in Europe⁵. SMEs are therefore facing an elevated financing and liquidity risk.

To reduce the financing risk, i.e. the risk that the company will be unable to finance itself, or pay too much for financing, or the liquidity risk, i.e. the risk of having insufficient liquidity to meet everyday variations in cash flows and working capital requirements, an SME needs to optimise capital allocation. Cash pooling solutions may assist SMEs immensely in this context.

Firstly, through a well-integrated, flexible tool with real-time visibility of consolidated cash positions, the organisation becomes more agile and capable of reacting to short-term liquidity issues. A consolidated view of cash positions allows the treasury to use idle cash resources, which may previously have remained unused, to fill short-term cash shortages.

4 European Commission, Annual Report on European SMEs 2013/2014

5 European Commission, Annual Report on European SMEs 2013/2014

The identification of idle cash resources may even permit the reallocation of treasury excesses into long-term capital, increasing available resources for long-term financing. Secondly, the automated sweeping capabilities of modern cash pooling tools will allow SMEs to reduce their interest charges by optimising cash positions.

This will help to improve the interest coverage ratio, which is increasingly used as an indicator by banks when evaluating potential loans. An efficient cash pooling solution can thus help companies to have financing more readily available.

By becoming international, SMEs enter a multibank, multi-country environment and operational risks linked to the treasury function increase

As the international presence of an SME becomes more pronounced, the governance of the different international presences becomes increasingly complex and difficult to control and the number of banks with which SMEs interact increases. Fraud risks, as well as the risk that processes or systems may fail increase.

Operational risks caused by a reduction in control, such as fraud risk, can be reduced through cash pooling solutions. Advanced cash pooling tools provide real-time visibility of all cash positions and cash movements and consolidate all activities in a central tool, which allows the centralised treasury to control and verify transactions. Optimally, banks will provide tools to SMEs that permit an integrated view of all accounts in a single flexible online tool, which is accessible at all moments. This should also integrate an overview of third-party banks and international accounts in the single tool.

This will be of particular use to SMEs, who typically have a strong link with one or two house banks. Moving into international markets will increase the number of banks with which SMEs will need to interact and new processes and systems are required.

As new systems and processes will not have systematically been tried and tested, there is a heightened risk of these failing. If the existing house bank can therefore provide an integrated tool showing all accounts with different banks, this can significantly facilitate the move towards a multi-bank environment for SMEs and reduce the risk. This additional service can furthermore contribute to further strengthening the relationship between the bank and the customer.

Conclusion

- In the context of globalisation and the aftermath of the financial crisis, SMEs are acting in a new competitive environment and facing new treasury risks
- To reduce their exposure to the new treasury risks, specifically market, financing and operational treasury risks, SMEs need new robust cash management tools
- Innovative cash pooling tools in particular can help to reduce the discussed risk exposure
- Considering the significant economic importance that SMEs have in today's economy, banks could benefit significantly from providing specific cash management tools to SMEs
- In order to capture the significant benefits associated to servicing the cash needs of SMEs, banks will, however, need to understand the particular needs of SMEs and adapt their offer to capitalise on their existing client base

Adopting a risk intelligent approach to pricing and capital needs for depositaries¹

Simon Ramos
Partner
Strategy, Regulatory
& Corporate Finance
Deloitte Luxembourg

Jean-Philippe Peters
Partner
Governance, Risk & Compliance
Deloitte Luxembourg

Arek Kwapien
Manager
Strategy, Regulatory
& Corporate Finance
Deloitte Luxembourg





Why is the risk and cost profile changing for depositaries?

Overview

The AIFMD regime introduced a range of new and more prescriptive requirements to harmonise depositary duties across the EU. In July 2014 the Luxembourg regulator, Commission de Surveillance du Secteur Financier (CSSF), published circular 14/587 focusing on UCITS depositaries, which heavily derives from the AIFMD's provisions and pre-empted the UCITS V obligations.

The main requirements of these regulations include daily monitoring of all cash flows, more frequent reconciliations and verifications, more robust due diligence and risk assessments, stronger segregation requirements and more detailed sub-custody oversight. Underlying these requirements is a change in the standard of liability, which firmly places the burden of proof on the depositary and makes it liable for loss of assets in the first instance.

¹ This article is largely based on the white paper 'AIFMD depositary pricing and capital: Taking a risk intelligent approach' available for download at <http://www2.deloitte.com/lu/en.html>

While depositaries have their own internal operational oversight and due diligence standards, the new regulatory frameworks covering alternative and UCITS funds require that all depositaries invest in operational realignment to varying degrees. In addition to the one-off investment required to align the depositary business with the latest regulatory requirements, increased responsibilities and liabilities have emerged.

It is the changing risk profile associated with the new duties and new liabilities that is likely to affect the depositary cost base and pricing to the greatest extent. Depositaries have sought to negotiate new contractual arrangements with prime brokers to mitigate or transfer ² this risk but will still be reliant on other parties in order to fulfil key duties.

Operational risks can be addressed through an enhanced control framework or increased automation. However, additional 'residual' risk will remain for depositaries, owing to the increased liability and the new depositary duties that have been defined. The key driver of cost and any increase in depositary pricing is therefore likely to be an individual risk premium based on a client's specific risk profile, as determined by the depositary.

While there is a diverse and evolving range of practices apparent in the market, we expect depositary pricing to focus increasingly on key risk factors such as contractual arrangements, automated reporting from other parties, network overlap with the prime broker, the location of assets and the complexity of arrangements/number of parties involved, for instance.

Depositary To Do List:

- Implement new cash flow monitoring requirements
- Implement new oversight controls on subs/reds accounts
- Implement new prime broker sub-custody reporting arrangements
- Ensure new asset segregation and reconciliation requirements are met at sub-custody level
- Implement new ownership verification and record keeping requirements and be able to produce a real-time inventory of OTC positions
- Increase due diligence and compliance monitoring of sub-custodians
- Increase monitoring of income distribution
- Monitor timeliness of settlements
- Increase frequency of valuation verifications
- Conduct a risk assessment of the AIF strategy and the AIFM organisation
- Implement look through on safe-keeping of financial instruments in custody
- Take action to mitigate liability risk

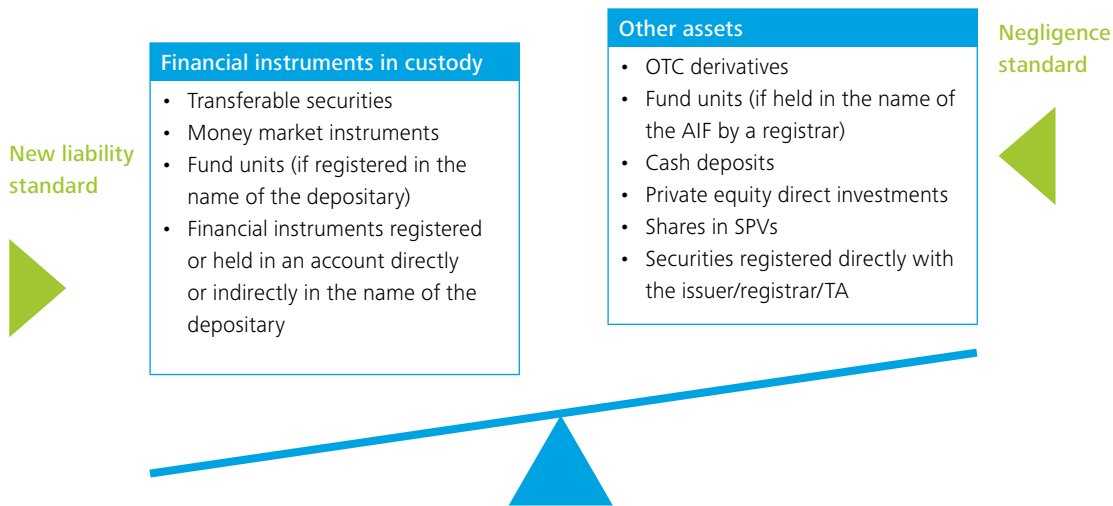
² Only applicable under AIFMD

Depository liability

Under the new regulations, the depository acts as a quasi-insurer for financial instruments held in custody. If such an asset is lost, the depository will need to make the fund whole without 'undue delay'. For 'other assets' that by their nature cannot be held in custody, the depository is subject to a best efforts 'negligence'

standard. Strict liability aside, depositaries face increased liability due to the risk of an error or breach in relation to the new range of more prescriptive duties they must fulfil. In addition, even for these non-custody assets, the bar has been raised via the imposition of new duties related to record-keeping and ownership verification.

Figure 1: Financial instruments subject to the new liability



The depository is liable for the loss of financial instruments held by both affiliated and unaffiliated sub-custodians. When under AIFMD a discharge of liability subject to strict conditions exists, CSSF 14/587 and UCITS V do not allow for any exception. Fraud, accounting errors, operational failures and failure to apply asset segregation requirements all count as 'internal events' falling under strict liability.

The depository remains liable for financial instruments held in custody that are passed from the Alternative Investment Fund (AIF) or UCITS to the prime broker, even though operationally it has no line of sight into the prime broker sub-custody network. All of these changes present significant operational oversight challenges and imply a change in the risk dynamic and, consequently, in the cost profile for depositaries.

Identifying risk factors and adopting the right response

The increase in depositary requirements under AIFMD, CSSF 14/587 and UCITS V calls for sound risk management approaches to properly identify, assess, manage, monitor and report the various types of risk faced by depositaries (operational, regulatory, financial, counterparty and reputational).

- Modification of how existing risks can materialise, i.e. the event(s) leading to the occurrence of the risk differ due to revised operating models. For instance, depositaries might have to adapt monitoring processes with respect to cash movements for private equity or real estate funds

The changes in risk profile can take various forms:

- New risks arising from new regulatory requirements and the consequential operational changes, e.g. new cash monitoring duties
- Increased exposure to pre-existing risks, e.g. increased liability for loss of financial instruments held in custody

Aligning risk responses with business strategy

Each depositary is expected to address the development of an AIFMD-compliant model differently. Responses can take various forms that can be categorised into four types – accept, mitigate, transfer or avoid – according to leading Enterprise Risk Management (ERM) frameworks such as ISO31000³, COSO-ERM⁴ and Deloitte’s Risk Intelligence^{TM5}.

Figure 2: Risk responses

Response	Definition	Examples
Risk acceptance	Deciding not to change the current situation and accept the risk exposure as it is considered to fall within the company’s risk tolerance. Acceptance entails no specific action, but also does not permit modification of the risk exposure	<ul style="list-style-type: none"> • Business as usual
Risk mitigation	Reducing the probability of occurrence or impact of a risk (or both) below an acceptable threshold. This is typically achieved through the improvement of existing controls or the addition of new controls. Mitigation may also include contingency, in the event that the risk still arises (e.g. the business continuity plan)	<ul style="list-style-type: none"> • Enhanced control environment • Enhanced capital buffer • Increased use of internal depositary network • Pricing strategy
Risk transfer	Shifting the threat of impact and ownership of response to a third party, by way of a contractual agreement between the two parties, typically through insurance policies or indemnification or risk transfer pricing	<ul style="list-style-type: none"> • Contractual arrangements • Extension of insurance policies • Pricing strategy
Risk avoidance	Eliminating the risk, or protecting the business activities from its impact, e.g. via a restriction of products or activities	<ul style="list-style-type: none"> • Complete market exit • Withdrawal from high risk sectors/markets • Avoid certain clients • Avoid dealing with certain third parties

3 www.iso.org/iso/home/standards/iso31000.html

4 www.coso.org/-erm.html

5 www2.deloitte.com/global/en/services/risk.html

There is no 'one-size-fits-all' solution. Responses are dependent on depositary-specific circumstances (e.g. the selected operating model) and strategic implications (e.g. the desired market positioning in the UCITS and alternative investment industry). Key questions need to be addressed at board level so that the resulting risk profile remains within an acceptable risk tolerance for the organisation. In practice, it is possible that certain depositaries will be willing to work outside of these target parameters if the commercial considerations on a client specific circumstance require it.

The board will need to consider the wide range of factors arising from changes dictated by the new wave of regulations when determining risk response strategies. Depositaries with limited exposure to AIFs and/or UCITS or with a book of relatively low risk securities could accept the risks as not material. Acceptance of risks may also be particularly desirable for organisations with greater risk-taking capacities or a higher level of risk tolerance. Depositaries that intend to maintain or build a significant presence in the fund market need to consider risk mitigation and risk transfer responses. These measures may include enhancing the control environment and/or adding further capital buffer (mitigate) as well as enhancing insurance cover, contractual structuring and/or adjusting the pricing strategy (transfer).

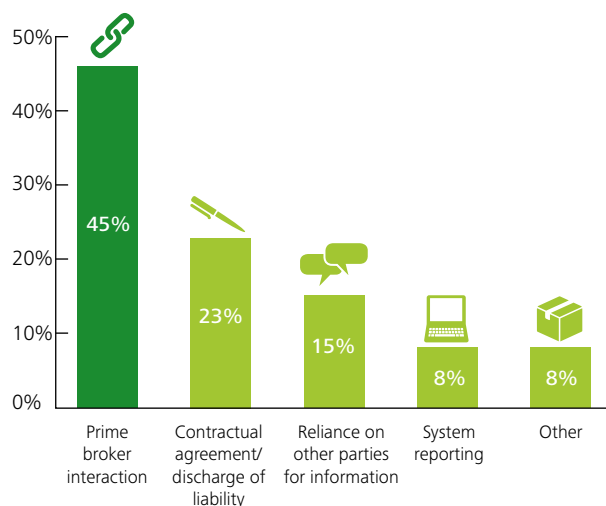
Responses will require an operational realignment in a way that maximises efficiencies and effectively manages risk in such a way that the business can maintain the optimum level of capital and competitive pricing. Developing the optimum target operating model is challenging and is typically achieved through a number of stages involving first stabilising, then optimising and finally transforming the business structure.

Key risk factors for depositaries

Depositaries need to map out all of the risk factors relevant to their business that arise from changes occurring under AIFMD, CSSF 14/587 and UCITS V.

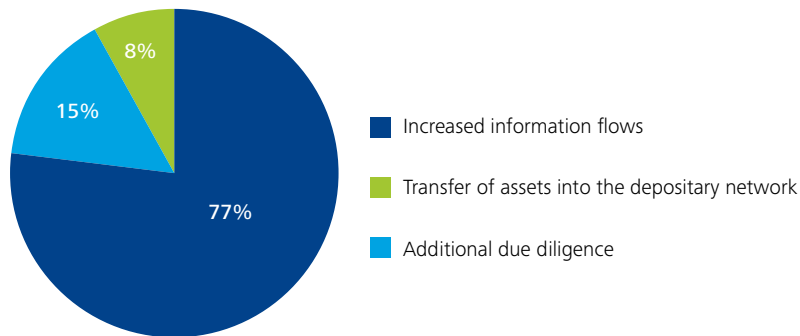
The requirements of the aforementioned regulations are closely aligned and so are the associated risks. In 2014, Deloitte conducted a survey of 14 major European depositaries on the pricing and capital impact of AIFMD⁶. Results indicated that almost half of depositaries rank interaction with their prime broker as their main concern, followed by contractual arrangements, reliance on other parties and system reporting.

Figure 3: Main AIFMD depositary concerns



⁶ See 'AIFMD depositary pricing and capital: Taking a risk intelligent approach', available for download at www2.deloitte.com/lu/en.html

Figure 4: What changes have you made, or are you planning to make in relation to prime broker interaction?



Prime broker and any third party custodian oversight demands a significant enhancement of the depository procedures and allocation of resources. The risk of potential liability for assets that cannot be identified within the prime broker's network and more generally throughout the safekeeping chain must not be neglected.

The depositories are therefore conducting additional due diligence on prime brokers, which in worst case scenario could result in a refusal to on-board a prime broker.

The increased oversight and reporting requirements also elevate the depositories' requests for information from prime brokers and other parties (e.g. collateral agents, clearing brokers, administrative agents).

Reliance on other parties for information presents a major challenge for depositories, in particular when other entities fail to supply the key data. Cash flow information is one of the examples where operational risk and challenges in receiving the information in a certain format, at a certain frequency and by a certain deadline imposes a considerable degree of risk.

Reliance on administrators within the group might pose fewer difficulties. It is therefore key to apply adequate contractual framework as well as operational flows and define an escalation process to allow for mitigation of these risks. System reporting is also of concern to depositories, due to the operational realignment involved and risks presented by a lack of automated reporting, including the proliferation of manual processes subject to more frequent errors.

Other issues identified in our survey which are causing concern for depositories include the application of segregation arrangements, operating in frontier markets (where segregation may be less developed), the number of prime brokers involved (risk multiplication factor and cost/ benefit ratio of on-boarding certain prime brokers) as well as the extent to which there is no network overlap. For the latter reason, depositories prefer to deal with familiar parties or entities within their group. Depositories will need to build such concerns into their risk profile, pricing and capital models in order to effectively manage risk.

Pricing strategy

Price factors

Custody and depositary fees are frequently set on a volume-basis offering low margins. This may not be commensurate with the level of financial risk exposure transferred to depositaries through increased liability and operational oversight, introduced by recent and forthcoming regulations. A potential misalignment of risk exposure and commercial incentives could have serious implications for a depositary, whose client base could become higher risk over time as prospective clients seek out the most competitive offering. On the other hand, clients with lower risk assets and custody arrangements will expect a fair price and justification for any price increase.

The way forward is through risk-adjusted pricing, based on individualised scoring in relation to a range of pre-determined risk factors, similar to the premium paid for insurance policies. While risk-based pricing is widespread in the credit activities of banks and in insurance policies, this kind of approach is less common in fee-driven businesses such as depositary services. Yet regulators increasingly expect institutions to adopt a risk-sensitive pricing mechanism that serves as an incentive to effectively allocate their financial resources in accordance with their risk tolerance and the principles of sound and prudent business management. The implementation of AIFMD is indicative of a trend towards risk-based pricing, as depositaries have sought to alert stakeholders to the cost impacts of the changing requirements. However, these assertions have rarely included quantifiable evidence.

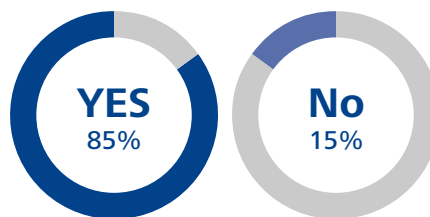
Depositary pricing could be influenced by three different drivers:

1. **Operational costs:** almost all depositaries needed to upgrade their existing capabilities to respond to new requirements, albeit to varying degrees. A certain amount of the operational and control realignment will include one-off investment costs that will not be recoverable from clients. These might include IT systems development or process re-engineering. Other recurring costs related to AIFMD and/or UCITS V, such as increased headcount or new activities will likely need to be considered in future pricing, given that business costs have increased. Our 2014 survey indicates that 85% of depositaries have increased (or plan to increase) their headcount as a result of AIFMD.

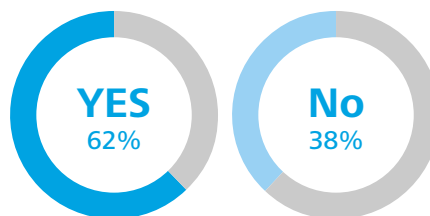
2. **Risk premium:** Depositaries should expect additional return where this involves taking on higher risks, whatever their nature. In classical risk models (such as those applied for credit risk), this additional risk is captured through the notion of 'expected loss'. Depositaries may need to build a range of factors into their pricing to adequately capture the risk premium. Further work may need to be done in this area as 62% of the depositaries we surveyed are developing a new pricing matrix to address liability and risk post AIFMD.
3. **Cost of capital:** The additional capital allocated to cover risks borne via the increased liabilities of the depositaries (equivalent to the notion of unexpected loss in credit risk models) implies a target rate of return that should be equivalent to what could have been earned if the depositary had chosen another investment with equivalent risk (i.e. the opportunity cost). In some cases, depositaries may need to bolster their capital reserves to cover the additional level of risk. Our 2014 survey suggests that over 60% of depositaries consider that AIFMD requirements impact on their internal capital requirements.

Figure 5:

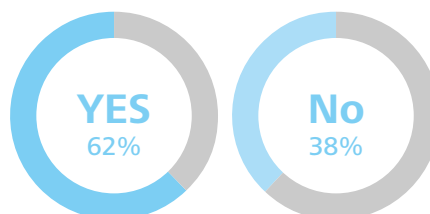
Do you plan to increase headcount as a result of AIFMD?



Have you developed a pricing matrix to take account of the new standard of depositary liability?



Do you consider that AIFMD depositary requirements impact your internal capital requirements to cover risks?



Commercial reality

Fully embedding all three elements (operational, risk and capital) into depositary pricing might not be entirely feasible for commercial reasons, combined with the complicated and difficult job of actually measuring risk premium and the level of capital to put aside for covering additional risk.

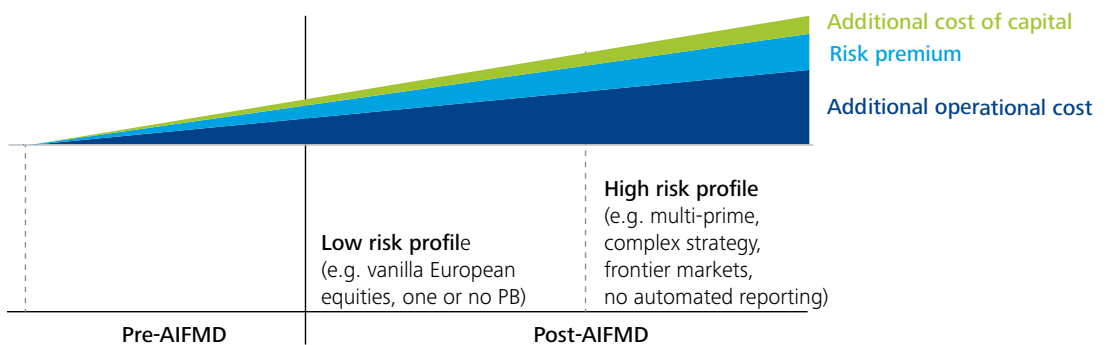
Indeed, the lack of historical experience and market quantification standards makes the calculation and pricing of this risk a challenging exercise. Currently, modelling the increased risk profile, capital needs and impact on price remains highly subjective and is still at experimental stage.

A diverse range of pricing practices and methodologies is apparent across the depositary industry. Survey respondents most frequently indicated contractual agreements, automated reporting, network overlap and number of prime brokers as factors they take into account in pricing, if they have developed a risk-adjusted pricing model in the first place. Other pricing factors cited include jurisdiction of the assets, type of assets, credit risk and whether the entity is affiliated.

Many of the factors clearly indicate a need to price risk sensitively when it comes to prime broker interaction. However, depositaries are mindful of the operational challenges regulation such as AIFMD creates for prime broker models. Thus, from a commercial perspective, depositaries are not generally seeking to drive operational change through pricing but rather through ongoing dialogue.

As a consequence, it is unlikely that new pricing strategy adopted by depositaries will encompass all three price drivers. This is especially true since many asset managers and management companies consider that the so-called depositary risks are actually existing risks that, while increasing with greater liability, should nonetheless already be compensated for by the existing control environment. By far the most impacting factor on the depositary fee adjustment cited in our 2014 survey was the additional risk premium (55%), followed by operational costs (36%), while only 9% plan to include increased capital costs in their AIFMD pricing.

Figure 6: Risk adjusted pricing (illustrative)



Risk intelligent pricing

While a great range of different practices and methods are observed in the industry, we advocate adopting a risk-intelligent approach to deriving the risk premium based on a set of key risk factors to differentiate the price applied to different funds.

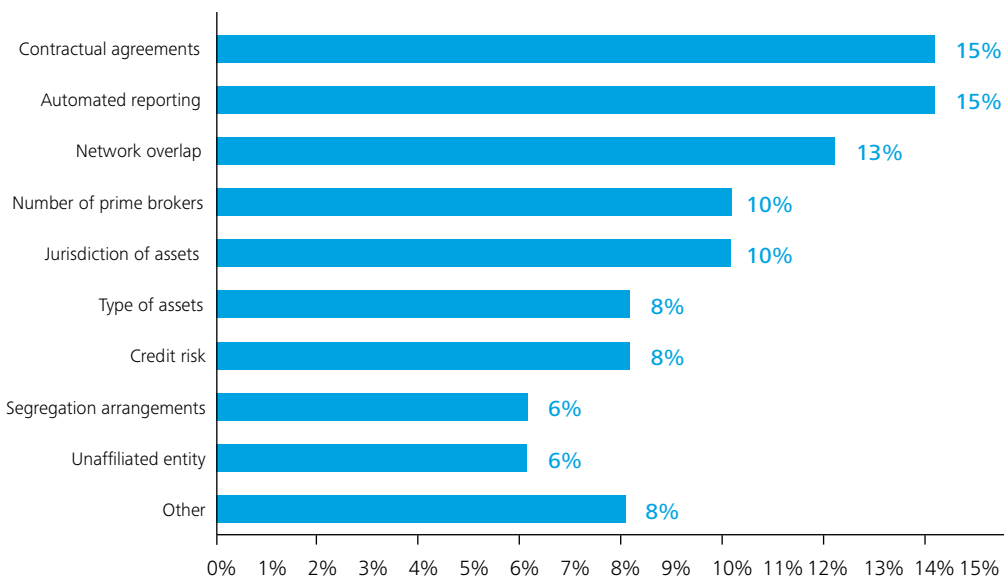
The approach is illustrated in the diagram ‘Calculating risk premium’: once relevant factors have been identified (step 1), risk factors are given a particular risk weighting (such as low, medium, high) to reflect the extent to which the client set-up exposes the depositary to errors or losses and the resultant financial exposure (step 2). Assessments of the risk factors are then aggregated to obtain an individual ‘risk score’ for each client (step 3). Finally this risk score is mapped against the level of maximum acceptable risk premium, so as to apply a price that will reflect the particular risk exposure implied by the operational set-up (step 4).

In the illustrative case presented in the diagram, the lack of automated reporting could be seen as a clear threat to a depositary, as it increases the likelihood of errors on a daily or weekly basis. The absence of automated reporting would therefore trigger a ‘high risk’ assessment for that particular risk factor.

Aside from sound risk management, this approach to depositary pricing will assist in raising awareness among sales functions of the critical risk factors that the depositary needs to address and will provide supporting evidence for justifying higher prices, where warranted by operational arrangements.

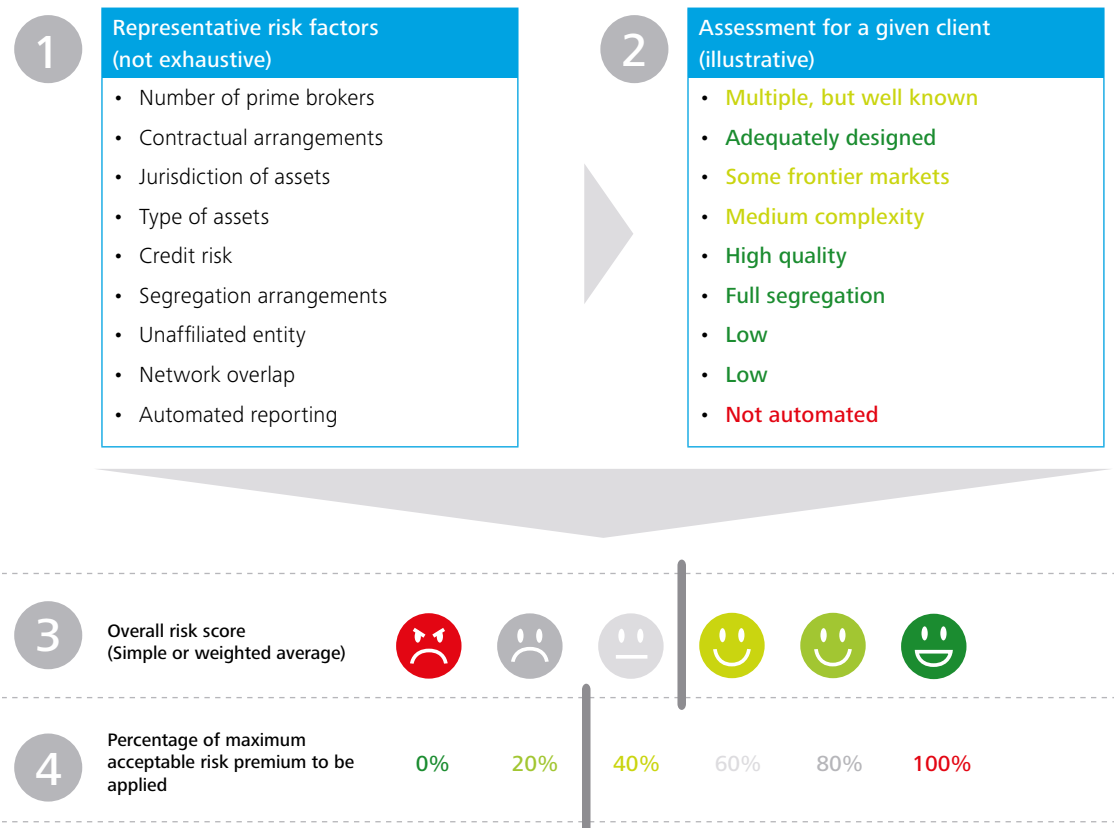
The methodology presented intentionally uses the notion of ‘maximum acceptable risk premium’, as it is evident that competition and market pressure play a central role in setting depositary fees.

Figure 7: Key depositary risk pricing factors



Source: Deloitte AIFMD depositary survey, based on percentage of respondents

Figure 8: Calculating risk premiums: Deloitte's view



Operational synergies

Large multinational institutions offering integrated solutions encompassing sub-custody and depositary services, affiliated prime brokers, fund administration, transfer agency services, cash management and corporate administration are best placed to offer lower pricing due to operational synergies across the group. At the other end of the spectrum, niche players in sectors such as real estate and private equity might also gain market share through aggressive pricing due to lower capital and operational costs from servicing non-custody assets only. Depositaries planning to increase price to reflect the impact of the modified risk profile on operating expenses and their capital base need also to reflect commercial realities and benchmark this decision against the competition and observed market practices.

Capturing AIFMD within internal capital requirements

Overview

Capital serves as a loss absorbency buffer for larger than anticipated (or unexpected) losses, as well as to fund the ongoing activities of the institution. The level of capital is a crucial market indicator for potential investors as well as rating agencies and other interested parties (including the general public). As a consequence, most financial institutions are required by their regulators to hold minimum amounts of capital. Banks and investment firms in particular are subject to the Basel framework transposed into the EU legislative framework through the Capital Requirements Directive (CRD).

The Basel/CRD framework requires institutions to hold a statutory minimum amount of capital to cover three types of risks:

- **Credit risk**
- **Market risk**
- **Operational risk**

Aside from the minimum capital requirements imposed by regulators (also called 'Pillar I measures'), institutions are also requested to perform a regular internal assessment of the amount of capital they need to hold to cover all the risks they face or could face.

The assessment therefore extends beyond the three types of risks listed above. This process, called the Internal Capital Adequacy Assessment Process (ICAAP), is forward looking and should encompass the expected evolution of activities and associated risks over the business plan cycle. The ICAAP is expected to paint a complete picture of the financial institution's risk profile. The senior management reviews this profile at least once a year and the board of directors approves the ICAAP report before submission to the competent authority for review.





Depository risks and the Basel/CRD framework

There is a market consensus that depository liability is best viewed in the context of operational risk, given the broad oversight responsibilities inherent in the new framework. A failure concerning one of the key new requirements relating to either safekeeping, oversight or cash monitoring would be of an operational nature, i.e. lack of adequate processes to ensure these obligations are met.

Depository liability would therefore be covered by an operational risk capital charge under the CRD regime and subject to Pillar I minimum requirements. Among the three approaches available to calculate these regulatory minimum requirements, the two simpler methods (the Basic Indicator Approach and the Standardised Approach) are solely driven by the institution's gross income and as a result do not reflect the specific operational risk profile of the institution. Only the Advanced Measurement Approach (AMA), based on internally developed models, is expected to offer sufficient granularity to reflect the impact of new regulation on the regulatory own funds requirements to cover operational risk.

However, this does not mean that only AMA institutions should be concerned about the capital implications of AIFMD. As seen above, new risks arising from changing regulatory requirements should be reflected in the ICAAP calculation, thereby impacting all depositaries subject to CRD.

Assessing the internal capital needed to cover increased operational risk exposures borne by AIFMD calls for an update and review of current operational risk and control mapping as well as of the stress test scenario analysis in place.

The delta method: Pre- and post-AIFMD assessment

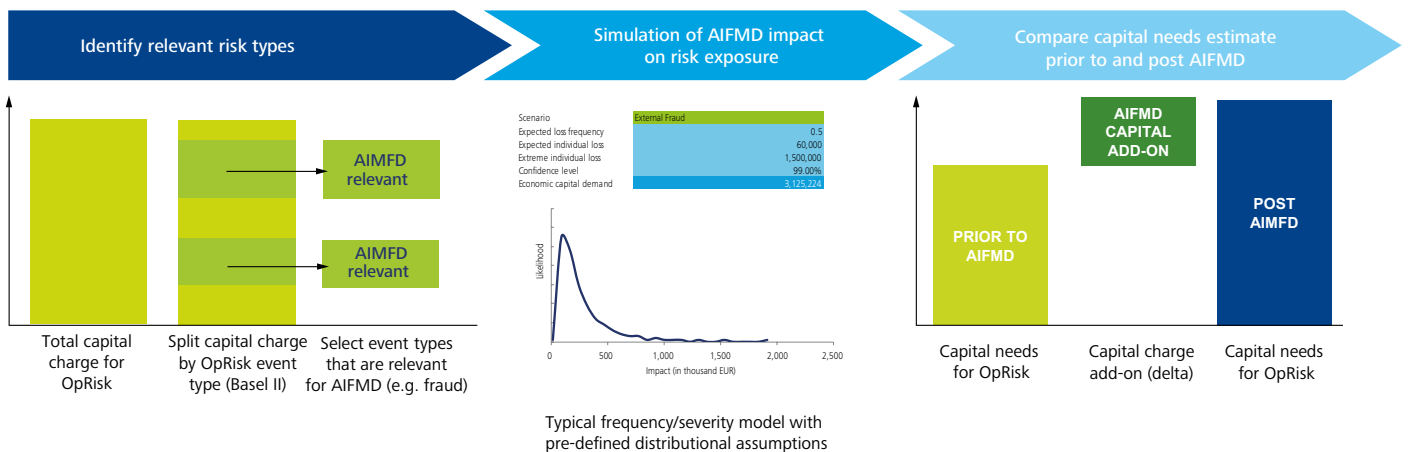
Operational risks related to the depositary function are clearly nothing new. An intuitive approach to assessing the impact of new AIFMD and/or UCITS V could work as follows: the operational risk profile would be assessed before and after application of the new rules (taking into account additional mitigation techniques such as strengthened controls for instance). If significant, the difference could be translated into dedicated additional capital needs. This approach is referred to as the delta method since it focuses on the variation or 'delta' of the operational risk profile when considering increased responsibilities under AIFMD/UCITS V.

- Identify operational risk event types that can be considered relevant from an AIFMD/UCITS V perspective
- Assess the impact of new requirements on both the likelihood of a given scenario occurring and the potential economic impact in case of such an occurrence
- Aggregate results and compare pre- and post-new regulations of internal capital requirement estimates

This approach requires the depositary to have an existing set of identified (and, ideally, quantified) operational risk scenarios to act as a starting point

The delta method is divided into three steps (also see the diagram below):

Figure 9: Overview of the 'delta method'



New risks arising from changing regulatory requirements should be reflected in the ICAAP calculation, thereby impacting all depositaries subject to CRD

Weaker internal controls would also lead to expanded capital needs, but to a much lesser degree than the operating model

Step 1: Identification

The first step is to identify which of the seven operational risk event types defined by the Basel Committee may be impacted by the new requirements. For instance, external fraud is evidently a factor to be considered from a depositary liability perspective, while employment practices and workplace safety would not be impacted by new rules under AIFMD or UCITS V.

Most of these scenarios do not actually relate to 'new' risk exposures but rather to 'increased' risk exposures. For instance, failure of a sub-custodian is not a new risk faced by depositaries, but the obligation to return assets 'without undue delay' to clients and the reversal of the burden of proof in the event of an issue lead to an overall increase in exposure to possible losses, penalties and charges. Consequently, there is an increased likelihood of an advance pay-out and the incident having greater economic impact resulting from dispute costs, inflation, market price fluctuations etc.

Step 2: Assessment

The second step involves undertaking an assessment of relevant risk scenarios and should account for management actions and new mitigation techniques, such as new or modified controls, implemented to address new requirements. This means that various end results are possible, including no change to the net risk profile if additional controls neutralise additional risk exposure.

In the 'sub-custodian failure' case described above, the impact on model parameters could be considered as follows:

- The likelihood that a failure of a sub-custodian results in an obligation to pay client claims increases
- The total economic impact of the scenario, including an advance pay-out and amplification of the impact due to dispute costs, inflation, market price fluctuations etc., is considered greater than previously

Quantification of the selected scenarios should then be performed by applying the classical frequency/severity model widely used in the financial sector. In smaller or less complex organisations, such modelling techniques might not be available to adequately quantify those scenarios. We believe that even with simpler approaches, this exercise remains a worthwhile contribution to an improved risk management process. Indeed, the key objective is for the outcome to be directionally correct, transparent to all stakeholders and consistent with regulatory requirements.

Step 3: Comparison

Whichever model is deployed, the last step of the process consists of comparing the outcome of the 'pre-AIFMD/UCITS V' assessment with the 'post-AIFMD/UCITS V' situation. The difference between both cases will form the basis for assessing the impact of new regulation on capital adequacy.

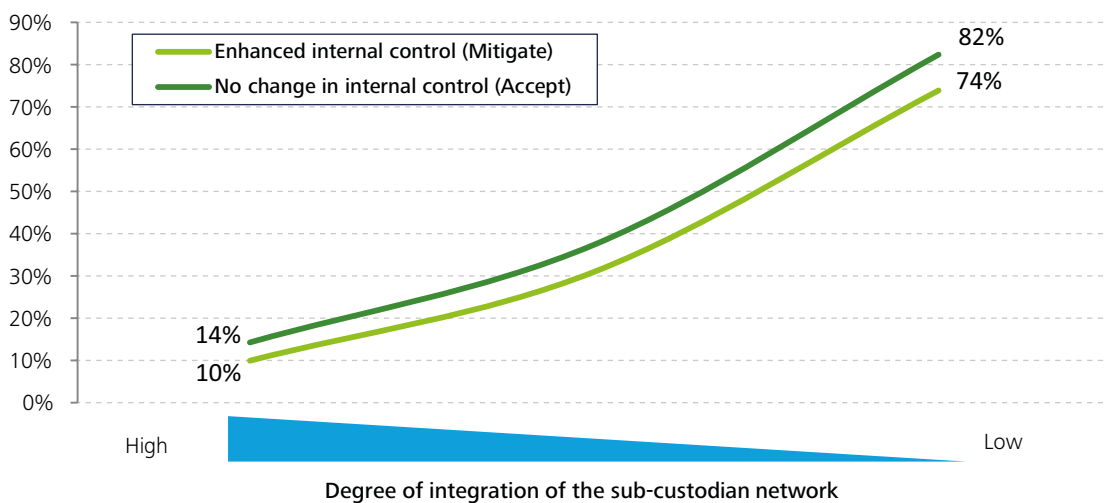
A Deloitte study⁷ illustrated this concept for AIFMD with a fictive case of a typical EU depository bank, based on operational risk data gathered by the Basel Committee, the ORX consortium, Pillar III disclosures and internal experiences. Key metrics of this fictive depository reflected a realistic order of magnitude observed among market participants.

Based on this initial set-up, the loss event types that were identified as 'relevant' for AIFMD are analysed and the impact on both frequency and severity is estimated. This impact is dependent on at least two key dimensions: (i) the degree of sub-custodian network integration and (ii) the strengthening of the internal control framework.

Simulations indicate a potential increase of capital requirements ranging from 30% to 38% for a moderately integrated depository bank. Such an increase of internal capital needs for operational risk could prove to be problematic, especially in institutions with a limited capital surplus.

This is particularly true for depositaries with limited sub-custodian network integration as our results indicate a high sensitivity to the operating model, with a potential increase in capital needs exceeding 70%. Weaker internal controls would also lead to expanded capital needs, but to a much lesser degree than the operating model, with an estimated increase of 4% to 9% in capital needs depending on the case.

Figure 10: Impact on internal capital requirements of new liability regime imposed by AIFMD relative to situation pre-AIFMD



7 'AIFMD depository pricing and capital: taking a risk intelligent approach', available for download on www.deloitte.lu.

Conclusion

European depositaries face an increased cost and risk profile as a result of AIFMD, UCITS V and, at the level of Luxembourg, of CSSF 14/587. Inevitably, some of these costs will be passed on to clients through pricing. Risk will be the biggest factor in determining pricing, followed by operational costs, while the capital impact on the price could be very limited.

The scale of the price increase should depend on a range of risk factors and depositaries need to develop more risk-sensitive pricing mechanisms to address this development.

Pricing must take into account a range of risk factors, which could expose depositaries to financial loss. These risk factors need to be weighted in importance in alignment with the organisation's risk appetite/policy. Each client needs to be assessed via the pricing model to give an accurate risk score and price. Failure to implement such a pricing model could lead to significant future losses and exposure to a riskier client base over the longer term.

Ongoing operational costs will also likely be reflected in the depositary pricing model to some extent, depending on the level of automation achieved and the increase in overheads such as staffing costs. Depositaries may only be willing to work with fund administrators within their group or may need to price more risk sensitively for conducting duties such as cash monitoring.

The issues in the centre of depositary attention are linked to reliance on other parties for information, segregation and safekeeping of assets. Oversight on these entities should be performed via initial and recurrent due diligence, setting up of dedicated agreements describing the roles and responsibilities of each party, putting in place KPIs/KRIs allowing for appropriate monitoring and defining an escalation process involving the fund management company (UCITS V mandatory requirement).

Depositaries' main concern, however, is how to fulfil obligations for in-custody financial assets held with prime broker or third party custodian and the associated operation of liability. UCITS V does not foresee a discharge of this liability, therefore many depositaries would strive to achieve an operational solution based on greater network integration over the longer term.

Combined with other regulatory initiatives (UCITS VI, EMIR, Target2 Securities, CSDR, MiFID II) focusing on custody/depositary services, clearing, settlement and reporting, further operational solutions that enhance data flows and mitigate risk will develop over time. Operational integration and the provision of data solutions are undoubtedly the business challenges but also the opportunities of the future.

Depositaries need to focus more on risk-adjusted pricing, based on individualised scoring in relation to a range of pre-determined risk factors







Operational risk

An emerging focus for investment managers

Edward T. Hida II, CFA

Partner

Global Leader - Risk & Capital Management

Global Financial Services Industry

Deloitte US

Investment managers may begin to shift their risk management focus back toward operational risk, as well as several other emerging areas, according to results from Deloitte Touche Tohmatsu Limited's (DTTL) *Global Risk Management Survey*, Eighth Edition, which gauged the state of risk management in the financial services industry, including investment management firms.



'The more evolved risk managers are examining the nuances of their firm's risk culture by devising new and improved ways to measure risk-taking throughout their organizations'

Cary Stier

Partner
Deloitte US
Global Investment
Management Leader
Deloitte Touche Tohmatsu
Limited

Most firms described themselves as effective in managing liquidity risk (85%), credit risk (83%) and regulatory and compliance risk (74%), according to survey results. However, only 45% gave themselves a high rating for operational risk management—a little less than the 47% recorded in the previous survey conducted in 2010. Eighty-six financial institutions from around the world participated in the survey, representing a range of financial services sectors and with aggregate assets of more than US\$18 trillion. One-half of the 86 respondents identified themselves as either stand-alone investment managers or investment managers of larger integrated financial institutions (primarily banks and insurance firms).

'These results underscore the inherent complexity of measuring and managing operational risk, and suggest that work remains to be done in this area,' says Cary Stier, vice chairman and Global Investment Management leader for Deloitte US. 'The more evolved risk managers are examining the nuances of their firm's risk culture by devising new and improved ways to measure risk-taking throughout their organizations,' he adds.

Indeed, *'the strategic importance of risk management and the potential for reputational harm can be seen in the 94% of respondents who indicated that their boards and/or executive management teams are spending more time on the oversight of risk compared to the last several years,'* says Garrett O'Brien, a principal at Deloitte US.

Emerging risks

Investment management firms are faced with three areas of emerging risks: model risk, IT security and cyber risk, and business continuity. Model risks are not limited to model-driven trading strategies, but also to quantitative models used for the purpose of valuation, trade allocation and risk management. Of the 61% of survey respondents who said model risk was included in their enterprise risk management (ERM) program coverage, only 50% believe they are effectively managing it. To address this type of risk, some investment managers are focusing their attention on model governance, model validation, deployment and maintenance.

'Cyber education can start with simple questions, such as who would want your information and why do they want it'



Mary Galligan

Director
Cyber Risk Services
Deloitte US

With 40% of breaches¹ resulting from hackers gaining access through third-party systems, it is increasingly important that investment managers understand their extended enterprise and the control frameworks that service providers have to secure client and transaction data as well as intellectual property. Some investment managers are conducting cyber threat assessments to better understand their potential exposure.

'Cyber education can start with simple questions, such as who would want your information and why do they want it,' notes Mary Galligan, a director with Deloitte US' Cyber Risk Services practice and former FBI special agent in charge of cyber and special operations. *'It's important for investment managers to start with a clear understanding of their vulnerabilities to make risk management and mitigation more informed.'*

Business continuity and disaster recovery continue to be a priority for the US Securities and Exchange Commission and a hot topic for the risk committee, in some cases being elevated to the board level. Many firms are re-evaluating or adjusting their strategies for dealing with extended disruptions, as recent natural disasters have provided a number of data points to gauge the actual effectiveness of existing plans.

Key risk management challenges

According to the Ponemon Institute's survey, a number of inhibitors to managing risk effectively are specific to investment management firms, including data and technology, resourcing and service provider oversight.

Data and technology

Investment management firms face significant system, infrastructure and data challenges, which are compounded by the investment manager's fund and account structures as well as by its reliance upon service providers for technology and data. The old adage, *'garbage in, garbage out'* still applies: Data quality is clearly affecting organizations' abilities to assess, monitor and mitigate risk.

¹ *'2013 Cost of Data Breach Study: Global Analysis.'*
Benchmark research sponsored by Symantec and independently conducted by Ponemon Institute LLC, May 2013.



Garrett O'Brien

Partner
Capital Markets
Deloitte US

'A key question emerging around managing risk in general is: what is the most efficient and effective way to focus their time and effort on risk, particularly if resources are constrained?'

Resourcing

Doing more with less is placing a premium on resources with the right skills to manage day-to-day risk while accommodating growing and emerging risk areas. *'For investment management firms,'* says Garrett O'Brien, *'a key question emerging around managing risk in general is: What is the most efficient and effective way to focus their time and effort on risk, particularly if resources are constrained?'* Increasingly, there is a shift toward allocating resources to key focus areas as a result of strategic risk assessments. The use of formal risk assessments allows organisations to compare and contrast risk exposures across areas that were traditionally managed in silos.

Service provider oversight

Financial firms face a variety of risks associated with their reliance on service providers, including theft, the inadvertent release of client-identifying data or the dissemination of intellectual property such as on strategy or trades and regulatory breaches. Some investment management firms are working to gain a more holistic view of their extended enterprise by evaluating the risk profile for each service provider. They are also establishing a service provider oversight framework that aligns with their overall risk profile.

The three views of assessing risk

Increasingly, investment management firms are taking an approach of characterising their risk in three views, which correlate directly to the levels of priority and focus of the board, executive management and risk committees:

- **Franchise threatening**
The 10 to 15 key risk areas that can threaten the reputation and operating ability of the firm
- **Regulatory imperative**
Fulfilment of fiduciary, regulatory, and legal responsibilities
- **Control environment**
All other risks, where the residual risk is understood and reviewed on a periodic basis against limits and acceptable losses

In addition, the more evolved risk managers are taking time to examine the nuances of their firm's risk culture by devising new and improved ways to measure risk taking throughout their organisations and stress the need for greater organisational awareness and integration across risk, IT, operations, compliance, internal audit and legal functions.

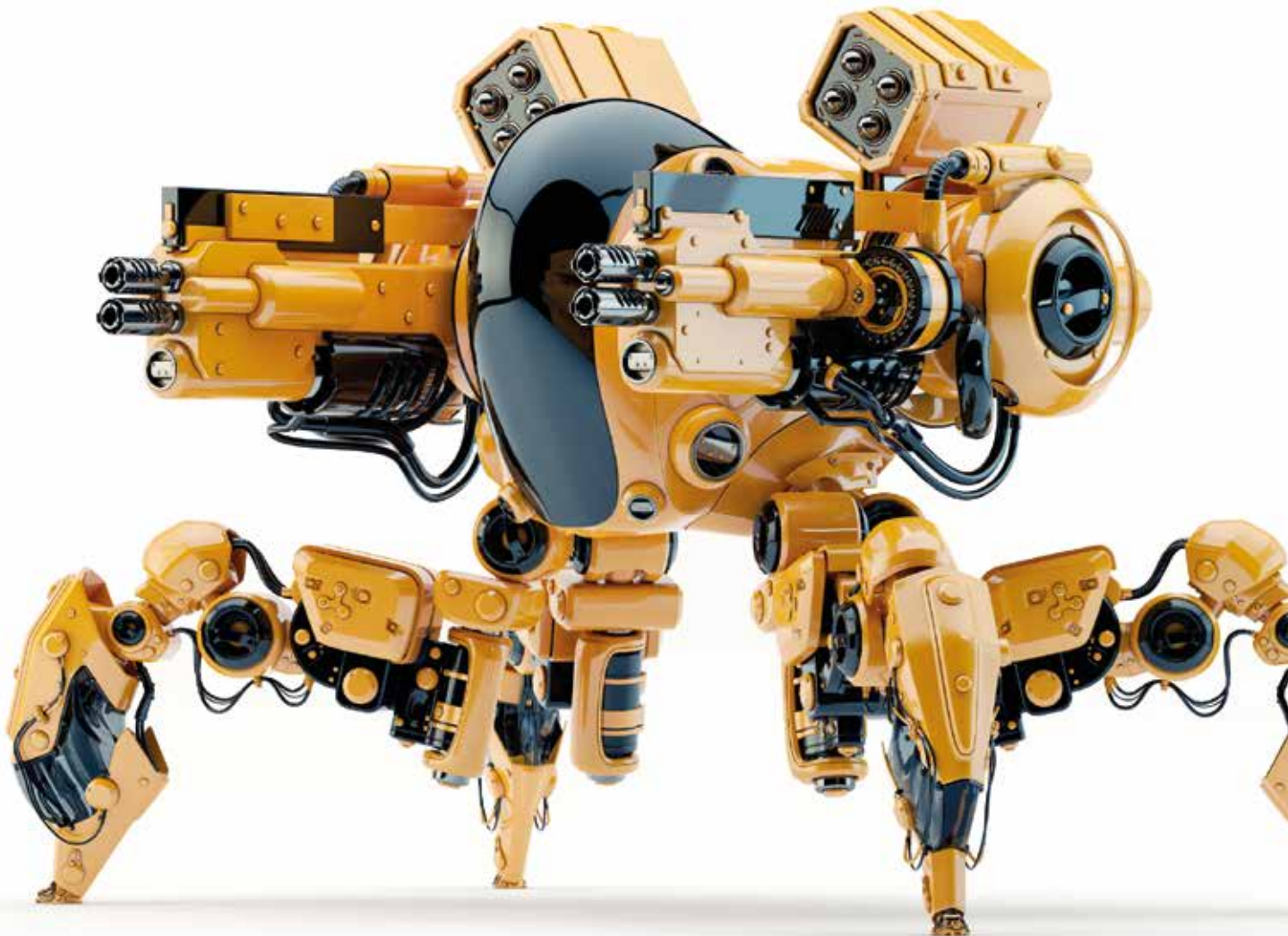


The use of formal risk assessments allows organisations to compare and contrast risk exposures across areas that were traditionally managed in silos

Global Cyber Executive Briefing Lessons from the front line

Stéphane Hurtaud
Partner
Governance, Risk & Compliance
Deloitte Luxembourg

In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many senior executives and board members, the concept of cybersecurity remains vague and complex.



Yet for many senior executives and board members, the concept of cybersecurity remains vague and complex. Although it might be on your strategic agenda, what does it really mean? And what can your organisation do to shore up its defences and protect itself from cyber-threats?

No industry or organisation is immune

A common myth is that cyber-attacks only happen to certain types of organisations, such as high-profile technology businesses. However, the cold, hard truth is that every organisation has valuable data to lose. In fact, the attacks that happen most frequently are completely indiscriminate - using scripted, automated tools that identify and exploit whatever weaknesses they happen to find. Cyber-attacks can be extremely harmful. Tangible costs range from stolen funds and damaged systems to regulatory fines, legal damages,

and financial compensation for injured parties. However, what might hurt even more are the intangible costs - such as loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, loss of integrity due to compromised digital assets, and overall damage to an organisation's reputation and brand - all of which can send an organisation's share price plummeting, and in extreme cases can even drive a company out of business.

What is the potential impact to your business?

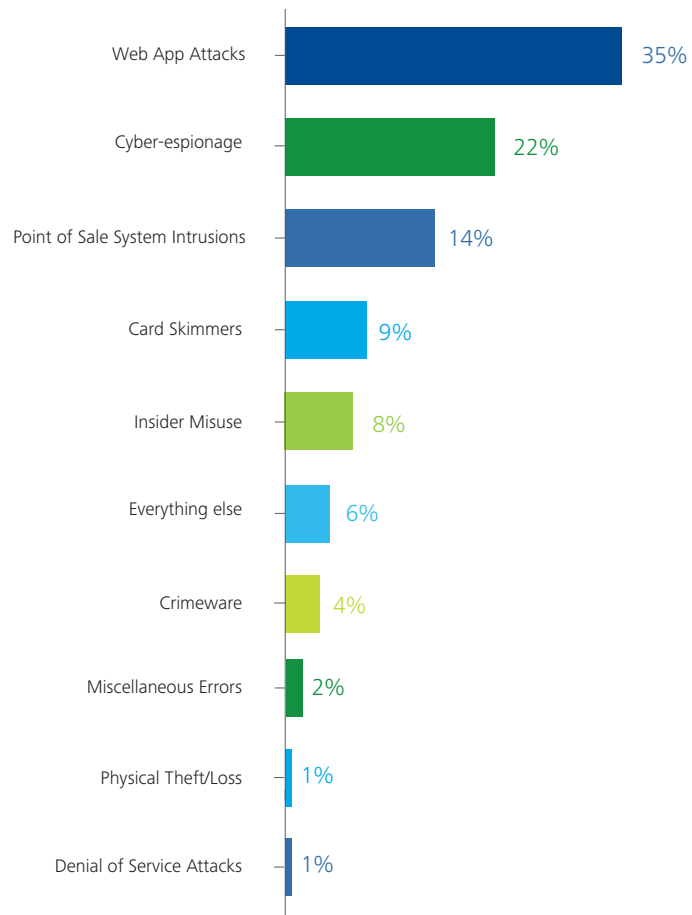
Being resilient to cyber-risks starts with awareness at the board and executive level; recognition that at some point your organisation will be attacked. You need to understand the biggest threats, and which assets are at greatest risk - the assets at the heart of your organisation's mission.

Who could potentially target your organisation, and for what reasons? Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack (see *Figure 1*), and what is the potential impact to your business?

Questions such as these can help determine how advanced and persistent the cyber-threats to your business are likely to be. This insight allows you, as a senior executive or board member, to determine your organisation's risk appetite and provide guidance that helps internal and external security professionals reduce your risk exposure to an acceptable level through a well-balanced cyber defence.

Who could potentially target your organisation, and for what reasons?

Figure 1: Frequency of incident classification patterns from 1367 breaches during 2013.



Source: Verizon 2014 Data Breach Investigations Report¹

¹ www.verizonenterprise.com/DBIR/2014/

The importance to understand the key cyber-threats for your industry sector

The Deloitte's 'Global Cyber Executive Briefing' report² is a starting point for organisations to understand their most important cyber-threats. It highlights the top threats for seven key industry sectors - retail, manufacturing, e-commerce & online payments,

online media, high technology, telecommunications, and insurance - and offers real-world stories and practical insights to help your organisation begin to assess its threat profile and stay a step ahead of cyber-criminals. Follow-on reports will highlight the top cyber-threats in other major sectors that are also highly vulnerable.

For those key industry sectors, the main highlights of the report include:

High Tech

The high-tech sector is often ground zero for cyber-attacks because (i) it has very valuable information to be stolen and (ii) the nature of high-tech organisations themselves. High-tech companies - and their employees - generally have a higher risk appetite than their counterparts in other sectors. Also, they tend to be early adopters of new technologies that are still maturing and are therefore especially vulnerable to attacks and exploits. In addition, many high-tech organisations have open environments and corporate cultures that are designed to stimulate creativity and collaboration, but are more difficult to defend. As a result, high-tech organisations typically have a very large attack surface to protect.

Online Media

The online media sector might have the greatest exposure to cyber-threats. Since its organisations operate online, they have a huge attack surface to protect. Also, since its products are in high demand and completely digital, there is a high risk of being infiltrated and robbed of valuable content - both by individuals and organised crime groups.

Telecommunications

Facing increased, sophisticated attacks, including by Government agencies using Advanced Persistent Threats (APT) to establish covert surveillance for long periods of time. Another critical threat unique to the telecommunications sector is the attack on leased infrastructure equipment, such as home routers from Internet Service Providers (ISPs).

E-Commerce & Online payments

Database breach (i.e. loss of customer data, including names, physical addresses, phone numbers) and online payment systems are vulnerable areas often attacked. Denial of service attacks also top the list, particularly by hackers who want to disrupt an organisation in a highly visible way.

Insurance

The sector typically has a lot of sensitive data to protect. Cyber-attacks are growing exponentially as insurance companies migrate toward digital channels with sophisticated attacks combining advanced malware with other techniques such as social engineering. While current attacks appear short-term, the report predicts the number of long-term attacks may be silently growing.

Manufacturing

Increasing in the amount of attacks by hackers and cyber-criminals as well as through corporate espionage. Types of cyber-attacks in manufacturing vary widely from phishing to advanced malware, targeting not only IT but also connected Industrial Control Systems.

Retail

Credit card data is the new currency for hackers and criminals. Insider threats in retail are increasing, giving rise to a new breed of criminals that focus on stealing information - especially the valuable cardholder data that flows between consumers and retailers.

² Full report available on: www2.deloitte.com/content/www/global/en/pages/risk/articles/Global-Cyber-Briefing.html

Breaches occur at all organisations - not because they are badly managed, but because hackers and cyber-criminals are getting smarter every day. By sharing information about breaches, we can learn how to better protect ourselves - an imperative being promoted by the Partnering for Cyber-Resilience³ initiative of the World Economic Forum.

The stories clearly show that breaches are inevitable: your organisation will be hacked someday. They also show that we all depend on each other for a resilient cyber-space. For example, online media can be used to spread malware; vulnerabilities in the high-tech sector affect other industries that use digital technology; and disruption in online payments impact e-commerce.

By sharing and understanding these cases and taking responsibility at the executive and board level, we can all work together towards a safer cyber-space.

Need for an effective and well balanced cyber-defence

The bad news, and as explained earlier in this article, is that cyber-attacks can result in significant tangible and intangible costs. The good news is that cyber-threats are a manageable problem. To be effective and well balanced, a cyber-defence must have three key characteristics: it must be secure, vigilant, and resilient:

- **Secure:** Being secure means focusing protection around the risk sensitive assets at the heart of your organisation's mission - the ones that both you and your adversaries are likely to agree are the most valuable.
- **Vigilant:** Being vigilant means establishing threat awareness throughout the organisation, and developing the capacity to detect patterns of behaviour that may indicate, or even predict, compromise of critical assets.
- **Resilient:** Being resilient means having the capacity to rapidly contain the damage, and mobilise the diverse resources needed to minimise impact - including direct costs and business disruption, as well as reputation and brand damage.

Although it is not possible for any organisation to be 100% secure, by focusing on these three key attributes, it is entirely possible to manage and mitigate cyber threats in a way that reduces their impact and minimises the potential for business disruption.



3 www.weforum.org/issues/partnering-cyber-resilience-pcr

To summarise, here are five takeaway questions to reflect on through the lens of a secure, vigilant, and resilient approach to cyber security:

1

Are we focused on the right things?

Often asked, but difficult to accomplish. Understand how value is created in your organisation, where your critical assets are, how they are vulnerable to key threats. Practice defence in depth.

2

Do we have the right talent?

Quality over quantity. There may not be enough talent to do everything in-house, so take a strategic approach to sourcing decisions. Are the security teams focused on the real business areas?

3

Are we proactive or reactive?

Retrofitting for security is very expensive. Build it upfront in your management processes, applications, and infrastructure.

4

Are we incentivising openness and collaboration?

Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal co-operation across groups and functions, and ensure that people are not hiding risks to protect themselves.

5

Are we adapting to change?

Policy reviews, assessments, and rehearsals of crisis response processes should be regularised to establish a culture of perpetual adaptation to the threat and risk landscape.

Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack?



Cyber Insurance as one element of the Cyber risk management strategy

Stéphane Hurtaud
Partner
Governance, Risk
& Compliance
Deloitte Luxembourg

Thierry Flamand
Partner
Insurance Leader
Deloitte Luxembourg

Laurent de la Vaissière
Director
Governance, Risk
& Compliance
Deloitte Luxembourg

Afaf Hounka
Senior Manager
Actuary Services
Deloitte Luxembourg

With the steady increase in cyber crime, many organisations across a variety of industries are susceptible to cyber attacks. Recent cyber attacks indicate that breaches are inevitable and can be extremely harmful. Cyber breaches can lead to tangible costs, brand degradation and changes in consumer behaviour.

In this context, many organisations have come to the realisation that a cyber attack is inevitable - it's not a question of 'whether' it will happen, but 'when'. Although it is impossible to be 100% secure, by developing a sound cyber risk management approach, organisations can implement a number of risk treatment measures for prevention, detection and response activities to keep cyber risks at an acceptable level. Furthermore, the ever-evolving cyber risk landscape is driving interest in cyber insurance as one complementary element of the cyber risk management approach, which allows organisations to transfer some of the risks associated with cyber incidents to their insurance provider.

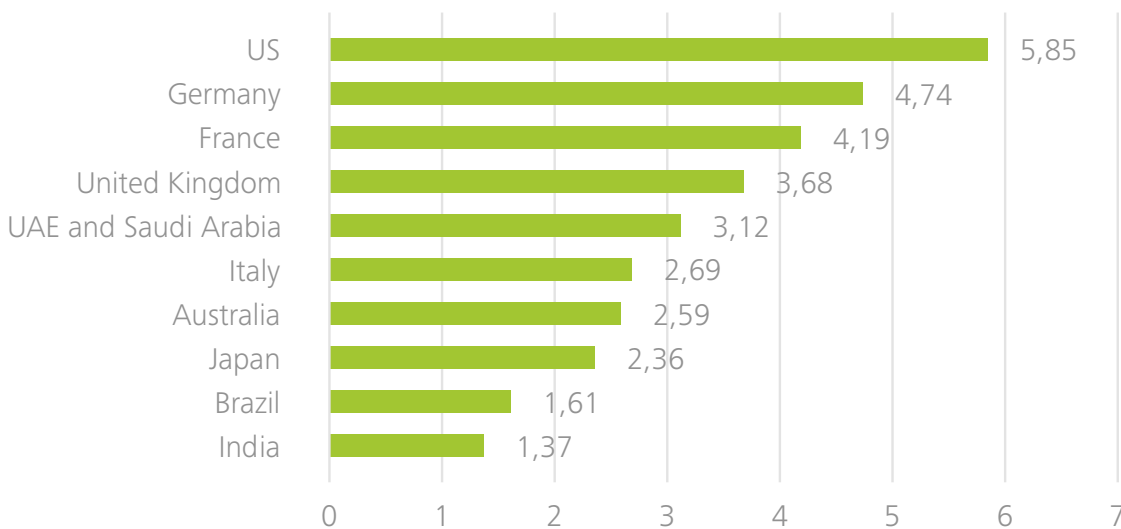
The cost of cyber crime

The largest data breaches in the last decade have cost each of the affected companies hundreds of millions of dollars.

- In 2014, the cost of a data breach ranged between US\$1.37 million and US\$5.85 million (depending on the country) (Fig. 1)
- Based on multiple analyst reports, the average cost per compromised record is anywhere from US\$78 to US\$277

The costs are attributable to investigation of the breach, remediation activities, notification of customers, credit monitoring, reputation management, legal fees and settlements, and regulatory fines.

Figure 1: Average total organisation cost data breach (measured in millions US\$)



Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute

Today's cyber insurance market

Cyber insurance can complement an organisation's active security measures by providing insurance coverage in three broad areas:

- Liability for a data breach or loss
- Remediation costs (e.g. for investigating the breach, notifying affected parties, etc.)
- Regulatory fines/penalties and settlement costs

The demand for cyber insurance, along with the number of insurance providers, has been increasing as the use of technology has become so prevalent.

The U.S. cyber insurance market accounts for approximately 90% of the global market¹, with annual gross written premiums estimated in the region of US\$2 billion for 2014, up from US\$1.3 billion in 2013². It is important to highlight that many early adopters were financial services companies, retailers and healthcare organisations with large amounts of personally identifiable information (PII).

The cyber security insurance market has developed far more quickly in the United States than in the EU because of the former's mandatory data breach notification laws. However, the European market can be expected to catch up over the medium/long term, as the coming EU General Data Protection Regulation (GDPR) will likely require prompt notification of personal data breaches to supervisory authorities.

Cyber insurance is only one element of risk management and it will never be able to remove cyber risk entirely

Despite the increase in cyber incidents, cyber insurance adoption among organisations remains at a low level: according to the 'Chubb 2012 Public Company Risk Survey', 65% of the publicly-traded companies surveyed do not purchase cyber insurance, yet 63% of decision-makers are concerned about cyber risk. This is primarily due to:

- **Lack of awareness** - many executives underestimate the costs associated with cyber incidents and/or inaccurately believe they are already insured under the firm's general liability policy
- **Underwriting complexity** - the increasing number of data breaches has led several insurers to become more cautious, and prospective cyber insurance buyers might be daunted by the complexity associated with the underwriting process (e.g. level of detail of risk surveys, potential use of third-party risk assessments, etc.)
- **The challenge of aligning insurance coverage with risk exposure** - broad expertise in IT and risk management is required to have a proper understanding of the total cost of cyber risk to an organisation and to determine whether the proposed terms and policies satisfy the organisation's needs

Overall, the cyber insurance market remains immature, with room for improvement:

- A wide range of coverage is on offer, and policies vary significantly from one provider to another
- There is limited actuarial data available for insurers to adjust premiums based on what security controls and products are most effective
- Coverage is inadequate in some areas, e.g. cyber insurance does not do a good job at covering intellectual property theft or reputational damage, and the downturn in business that may result






¹ Gartner Inc.



² The Betterley Report: Cyber/Privacy Insurance Market Survey 2014, Betterley Risk Consultants

Coverage provided by cyber insurance

Although traditional insurance policies may offer the option to cover some specific areas related to cyber risk, they are not designed to fully cover all the potential costs and losses.

Figure 2: Comparison between traditional insurance and cyber policies

	General liability 	Property 	E&O/D&O 	Crime 	Cyber 
Network security	+	+	+	+	✓
Privacy breach	+	+	+	+	✓
Media liability	+		+		✓
Professional services	+		+	+	✓
Virus transmission	+	+	+	+	✓
Damage to data	+	+	+	+	✓
Breach notification	+		+	+	✓
Regulatory investigation	+		+	+	✓
Extortion	+		+	+	✓
Virus/hacker attack	+	+	+	+	✓
Denial of service attack	+	+	+	+	✓
Business interruption loss		+	+		✓

 Possible
 Coverage

Cyber insurance policies provide a variety of coverage options and pre-conditions that need to be considered when purchasing cyber insurance:

- First party coverage protects against losses incurred directly by the company in response to a cyber incident (direct expenses), and typically includes theft and fraud, forensic investigation, business interruption, extortion, and computer data loss and restoration
- Third party coverage: protects against losses incurred by third parties in response to a cyber incident, and typically includes litigation, dealings with regulators, notification costs, crisis management and credit monitoring

Cyber insurance is written and priced to suit individual customers. As such, cyber insurance policies may stipulate exclusions, impose limits, or add clauses to protect the insurer from higher risks

(e.g. non-performance of a cloud-computing provider, unencrypted devices that contain personal or other sensitive data, computer software malfunctions due to programming errors.)

In general, cyber insurance cannot provide:

- Protection from reputational risk - while a monetary claim can be awarded for an information security breach, the damage done to an organisation’s brand cannot be repaired as easily or transferred to an insurance carrier
- The removal of risk - insurance, whether cyber or otherwise, provides the organisation with the opportunity to transfer, not remove, risk
- A replacement for an information security programme - strong security controls and a comprehensive information security programme are prerequisites for purchasing cyber insurance

Figure 3: Typical premiums for cyber insurance

Size of Company (Based on Revenue)	Small Companies (Less than \$100 Million)	Midsized Companies (\$100 Million - \$1 Billion)	Large Companies (More than \$1 Billion)
Coverage	\$1 – 5 million	\$5 – 20 million	\$15 – 25+ million
Yearly Premium (Cost for Coverage)	\$7,000 – \$15,000 per million in coverage	\$10,000 - \$30,000 per million in coverage	\$20,000 - \$50,000 per million in coverage
Typical Coverage Sublimits (Restrictions on Payout)			
Sub-limits can restrict payouts on a single aspect of coverage from 10 – 50% of the total coverage			
Notification Cost	\$100,000 - \$500,000 limit	\$500,000 - \$2 million limit	\$1.5 - \$2.5 million limit
Crisis Management Cost	\$250,000 - \$1.25 million limit	\$1.25 - \$5 million limit	\$3.75 - \$6.25 million limit
Legal and Regulatory Defense Expense	\$500,000 - \$2.5 million limit	\$2.5 million - \$10 million limit	\$7.5 - \$12.5+ million limit

Source: Deloitte research on insurance provider Web sites

As an example, consider a large credit card processor that purchased a cyber insurance policy with coverage of US\$30 million against a cyber incident. Unfortunately, a data breach involving several million credit cards resulted in the company paying over US\$145 million in compensation for fraudulent payments. In this situation, the insured party had to pay out US\$115 million and was not adequately covered.

In order to gauge the cyber coverage organisations need more effectively, insurers have started to implement a more rigorous procedure for underwriting cyber insurance policies.

This procedure includes a number of well-defined steps:

- **Initiate** - the cyber insurance broker/provider asks the customer to complete a self-assessment form on its information technology (IT) and security environment
- **Assess** - the cyber insurance provider reviews the assessment, then arranges an onsite assessment of the customer. For higher risk customers, the cyber insurance provider requests a third-party risk assessment to be performed on the customer, with the cost charged to the customer
- **Review** - the third-party risk assessment partner provides the results to the cyber insurance provider based on baseline IT and leading security practices
- **Report** - the cyber insurance provider uses the third-party risk partner's recommendations to produce its own assessment report
- **Underwrite** - the cyber insurance provider finalises the coverage and any exclusions, and calculates the premiums based on its assessment report

Key considerations for selecting cyber insurance

When selecting a cyber insurance policy, we recommend paying attention to the following considerations:

Understand your organisation's risk exposure

- Evaluate your current cyber risk exposure to understand the type and amount of cyber insurance coverage required
- Coverage may not be required in areas where controls are well established and routinely tested

Understand policy complexities

- There are a wide variety of insurance policies available, often requiring a rigorous underwriting process - spend time upfront understanding the pre-conditions that need to be met in order to obtain insurance
- It is also important to understand any policy exclusions to make sure that you are able to take advantage of the coverage you will be paying for

Balance the cost of premiums and of implementing controls

- While insurance policies may assist in transferring risk, organisations should conduct a cost-benefit analysis to determine the appropriateness of investing in cyber insurance coverage
- Make sure you are buying cyber insurance to cover the risks that cannot be addressed in-house

Understand the claims process

- Not all cyber claims are treated equally - know what will be needed to file a claim and make sure you can satisfy these requirements before purchasing insurance
- When an incident happens, insurers often require organisations to execute a formal incident response process - including saving logs, emails, forensic scans and other evidence - using methods that preserve the integrity of the evidence

Cyber insurance products are no replacement for a robust information security programme.

Cyber insurance is only one element of risk management (i.e. risk transfer), and it will never be able to remove cyber risk entirely. Organisations should first develop mature information security programmes and an understanding of the total cost of their cyber risk before seriously considering cyber insurance.



Becoming 'Reactively Proactive' Rethinking compliance risk management in today's environment

J.H. Caldwell
Partner
Regulatory &
Risk Strategies
Deloitte US

John Graetz
Principal
Governance, Regulatory
& Risk Strategies
Deloitte US

Thomas Nicolosi
Principal
Enterprise Risk Services
Deloitte US

Susan Jackson Redman
Senior Manager
Enterprise Risk Services
Deloitte US

Anna Blythe Papson
Manager
Enterprise Risk Services
Deloitte US

Joanna Connor
Senior Manager
Enterprise Risk Services
Deloitte US

Introduction

In light of recent and ongoing changes in the global financial markets, there is a significantly increased focus on the supervision and regulation of the financial services industry. Changes in existing laws, rules and regulations, together with new requirements and regulatory expectations, are likely to have a material effect on a financial institution's operating model.

The global regulatory environment has been and continues to be fluid and increasingly complex as a result of regulatory reform. Financial institutions are faced with a number of new regulatory obligations, tougher restrictions on risk taking, greater day-to-day direction by regulators, increased scrutiny of reliance on third parties and increased costs for compliance.



The regulatory changes are largely the result of the following factors:

- **Supervision:** The new environment is more prescriptive, less flexible and less predictable
- **Legislation and regulation:** The regulators are focused on reducing risk through the enhanced prudential standards, an orderly resolution scheme and greater consumer protections
- **Focus on operational processes that give rise to regulatory risks:** Regulators have clearly stated an expectation for increased oversight of operational risks, particularly where operational failures increase compliance risk and impact consumers
- **Enforcement:** The regulatory culture has become more enforcement driven as a result of the financial crisis, including enforcement surrounding consumer and trading related activities
- **Global regulatory coordination:** Regulators are collaborating more across borders to ensure that they have a comprehensive supervision strategy

This environment is creating a new challenge for the executive management and boards of financial institutions, which must come to terms with the new reality of compliance. What is the size and shape of the compliance infrastructure (e.g. people, process, and technology) they need to have in place to remain compliant – and avoid the major fines and reputational risks that come with enforcement?

Is the entire organisation acting in a consistent and strong manner when it comes to compliance? These are the types of questions many financial institutions have been wrestling with recently. As a result, the outlines of a new compliance framework have begun to emerge and take shape. In this article, we will describe some of the many important tools and considerations being used by industry leaders as they respond to more stringent and forceful regulatory scrutiny.

Find your baseline: strategic self-assessment

A starting point for a financial institution in determining its compliance with all laws, rules, regulations and regulatory guidance is to perform a strategic self-assessment of the overall compliance risk management programme in light of the new global regulatory environment. For many organisations, this is a common technique used today; however, few have actually undertaken the effort required to proactively assess their level of compliance with regulatory guidance, largely because 'knowing' has not been mission-critical. Today, what you do not know may hurt your organisation and many financial institutions find themselves becoming reactively proactive to stay ahead of the regulators.

Several whitepapers from the Basel Committee on Banking Supervision (BCBS), including *Compliance and the Compliance Function in Banks (BCBS 113, April 2005)*, *Principles for Sound Management of Operational Risk (BCBS 195, June 2011)* and *Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239, January 2013)* as well as resulting guidance by various home country regulatory agencies have arguably evolved certain regulatory principles into outright requirements. As a result, many financial institutions have implemented compliance risk management frameworks to address them. However, many financial institutions' execution of these frameworks has been viewed by the regulators as being inadequate in meeting the heightened regulatory standards.

The shortfalls often involve weaknesses in establishing independence for compliance management and staff and decisions around the adequacy of the compliance budget, compensation for personnel, performance evaluations, compliance testing, training, policies, procedures and effective escalation of compliance issues. These can impact the financial institution's ability to effectively aggregate, analyse, report and holistically address compliance issues across the enterprise.

Strategic self-assessments can be important tools for identifying and assessing how compliance risks are being overseen at both the line-of-business and enterprise levels. In addition, they can be critical in helping organisations prepare for internal audit and regulatory examinations by assisting in proactively identifying issues and non-compliance and allowing for time to address such issues prior to examination start dates. When performing a self-assessment, it is prudent to anchor regulatory guidance to business/enterprise controls and processes, which helps to provide additional insight and transparency of where requirements are being met (or where they are lacking) within an organisation.

The self-assessment may be used as a basis for analysing certain aspects that are key components for a compliance program framework (see *Figure 1*). These key components include governance, risk assessment programme and controls, policies and standards, compliance monitoring and testing, reporting and communication, compliance training, compliance technology as well as regulatory interaction and coordination. With respect to these components, there appear to be emerging and common industry challenges towards designing and executing effective compliance programmes.

These challenges underscore the focus of the BCBS 113 compliance principles and include among others:

- A firm-wide approach to compliance risk management that generates meaningful compliance risk information and analysis capabilities, not just static reporting
- Formalised and systematic processes and clear responsibilities and accountabilities to support independent compliance oversight
- Comprehensive and risk-focused compliance monitoring and testing that evaluates control effectiveness as well as compliance with laws and regulations
- Analysis and reporting tools to facilitate effective board and senior management oversight

Figure 1: Critical components of a robust regulatory compliance risk management programme





In reality, the cost center-view of compliance is quickly becoming outdated as compliance becomes increasingly enmeshed with core business strategy.

It is hard to imagine accomplishing any strategic goal without incorporating regulatory compliance. In fact, a strong compliance function can help an organisation gain competitive advantage by mitigating legal and reputational risks and further unlocking value through efficient and effective risk management. So after taking the important step of self-assessment, there is another fundamental question to answer: How do we take the assessment of our current state of compliance and leverage that information to build our future-state vision and goals? Building an in-depth strategic plan is the next critical step.

The strategic plan for compliance is a formalised vision and strategy for the compliance function – one that answers familiar strategy-level questions such as:

- What does our compliance function seek to achieve?
- What is the mission and vision of compliance?
- How will compliance support core business goals?
- Is there an opportunity to drive further cost efficiency through the use of technology and tools?

It is also important to remember that this is a strategic plan only for compliance risk, not risk management overall. An organisation may already have a strategic vision for risk management. But compliance risk is so important today that it warrants its own compliance-specific strategic plan with the overall vision of the organisation considered in the context of compliance-specific development needs.

In addition to providing the organisation with significantly increased clarity on the desired role of the compliance function, such a plan can be a useful tool in communicating with regulators. Regulators recognise that to maintain or become compliant in a radically changed environment is a challenging proposition that will not happen overnight with the waving of the proverbial magic wand. Besides the fundamental core day-to-day compliance activities, regulators also want to know that an organisation has a plan for getting there – along with the board and executive team. The strategic plan certainly may help.

Make the map: Strategic planning

Once an organisation has determined its baseline and identified any compliance programme gaps, the next step is to build a strategic plan. Banks have no shortage of strategic plans in place, but when it comes to compliance, there is often comparative radio silence. For many, that is largely due to the fact that the compliance function is viewed as less important than a growth-oriented, profit-driven line of business. To quote Susan Bies, former U.S. Federal Reserve Board governor and now board member for a top-tier U.S. financial institution, *'A culture of compliance should establish—from the top of the organization—the proper ethical tone that will govern the conduct of business. In many instances, senior management must move from thinking about compliance chiefly as a cost center to considering the benefits of compliance in protecting against legal and reputational risks that can have an impact on the bottom line.'*¹

¹ Bies, Susan Schmidt, 'Enterprise-Wide Compliance Programs,' Remarks at the Bond Market Association's Legal and Compliance Conference, New York, NY, February 4, 2004. <http://www.federalreserve.gov/boarddocs/speeches/2004/20040204/default.htm>

All about execution: The action plan

Once the strategic plan has been built, detailed actions and milestones for executing the plan should be defined and documented via an in-depth action plan. The action plan should address gaps identified during the self-assessment process, actions required for implementation of the strategic plan and any open regulatory findings pertaining to the financial institution's management of compliance.

Associated target completion dates for each action should be identified. These dates should be heavily considered and discussed prior to being documented, as it is likely that the action plan will be shared with internal audit and the regulators and dates will be socialised, especially if there are any open regulatory findings related to any actions.

In addition, specific executives should be made accountable for each action. Demonstration of executive accountability and tone at the top is key in satisfying regulatory expectations and, perhaps even more importantly, when organisational transformation is underway to win the support of financial institution's associates. It is critical that associates experience the commitment to change, as their willingness to play an integral part in the operationalisation of the financial institution's strategic plan and target operating model is vital for the success of the future-state vision.

Effective execution of the action plan will typically lead to the revision of various elements of the enterprise compliance programme such as governance, compliance risk management committees, global compliance policy and procedures, risk assessment process and monitoring as well as testing methodology and plans.

This will not happen overnight

It takes time to move the needle on compliance in a new environment like the one financial institutions face today. There are new policies and procedures to be developed and implemented, process and technology impacts to address across the organisation. Nevertheless, the only way to gain momentum is to begin making some moves, no matter how small. In this case, the place to start is with the self-assessment. Just remember that the assessment is an important commitment that will undoubtedly uncover important gaps to be addressed.

Many could say that this exercise is not just a nicety. A new approach to managing compliance risk is necessary and is now a more-important-than-ever component of a growth plan.

What a typical strategic plan should look like

While there is no official view on what a strategic plan should look like, the content listed below offers a good guide as to what key components should be considered. As you can see, the intent of the plan is to go well beyond a gap analysis. It should be a practical, strategic guide to compliance risk management.

- Executive summary
- Mission statement
- Vision statement
- Global regulatory environment
- Current-state observations
- Future-state vision



FATF Guidance

Transparency and beneficial ownership

Michael JJ Martin
Partner
Governance, Risk
& Compliance
Deloitte Luxembourg

Eric Collard
Partner
Governance, Risk
& Compliance
Deloitte Luxembourg

Irène Sanna
Analyst
Governance, Risk
& Compliance
Deloitte Luxembourg

Countries whose national laws do not contain provisions on trusts or which do not recognise trust or similar legal arrangements are not exempt from obtaining information on beneficial ownership of trusts

Introduction

On 27 October 2014, the Financial Action Task Force (FATF) adopted a Guidance on Transparency and Beneficial Ownership. FATF Guidances assist the interpretation of the FATF Recommendations, which set international standards against money laundering and terrorism financing (ML/TF). The Guidance aims at assisting policy makers and practitioners in national authorities in the implementation of FATF Recommendations 24 (Transparency and Beneficial Ownership of Legal Persons) and 25 (Transparency and Beneficial Ownership of Legal Arrangements). Corporate vehicles are used to conduct and facilitate business activities, but they can be misused to launder the profits of illicit activities. The misuse of corporate vehicles for illicit activities can be reduced and prevented if information on the underlying persons conducting the business is easily accessible by the competent authorities.

The misuse of legal persons and arrangements and the definition of beneficial owner

Relevant studies have demonstrated the misuse of legal persons and arrangements for the purpose of concealing the identity of criminals, the purpose of assets held by corporate vehicles and the source or use of the funds through instruments such as shell companies, complex ownership and control structures, bearer shares etc. Moreover, when complex legal structures involve multiple jurisdictions, slow international co-operation may frustrate the recovery of

the information. Lack of legal obligations on companies and trusts to provide information on the beneficial owners contributes to a higher risk of using legal persons and arrangements for the purpose of ML/TF.

The definition of beneficial ownership provided by the FATF Recommendations in the context of legal persons refers both to the person who ultimately owns the legal entity, as well as to the person who can take relevant decisions within the legal entity. The notion mainly focuses on identifying the natural person who actually owns and takes advantage of the assets held by the legal person; it also includes natural persons on whose behalf transactions are conducted. In the context of legal arrangements, the FATF Recommendations identify the beneficial owner as the natural person who ultimately owns or controls the legal arrangement and who exercises control over the legal arrangement.

Effective mechanisms to combat the misuse of legal persons and arrangements

In February 2013, the FATF has developed a system to assess to which extent financial systems and economies are protected from the risks of ML/TF, using eleven Immediate Outcomes. When a financial system complies with Recommendations 24 and 25, the country's AML/CFT system is effective, therefore *'legal persons and legal arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments'* (Immediate Outcome 5).

Enhancing transparency of legal persons – Recommendation 24

Recommendation 24 applies to all legal persons including companies, foundations, partnerships, associations and any type of entity that can own property and enter into a customer relationship with a financial institution.

1. Initial obligations

In order to enhance transparency of legal persons, countries should adopt appropriate measures for each type of legal entity, based on a risk-based approach; moreover, countries should ensure that competent authorities have access to the information in a timely manner. Examples of appropriate measures to enhance transparency of the legal persons are: identification of the type of entity and of its basic characteristics; identification of the process of creation of the entity and identification and registration of the data on the beneficial owner of the legal entity; public availability of the identified information; assessment of the correspondent ML/TF risks related (including risks related to specific jurisdictions and to specific types of services provided).

2. Enhancing transparency

After setting obligations, countries should implement measures to enhance transparency of legal entities. This process entails two main features: obtaining basic information on the legal entities and obtaining information on the beneficial owners of the entities.

- **Basic information**

Obtaining basic information on the legal entities comprises two steps.

Firstly, each country should have a company registry that contains publicly available basic information on the companies (e.g. name, proof of incorporation, legal form and status, registered address etc.). Secondly, legal entities should collect and record basic information on the entity itself (e.g. name, proof of incorporation, legal form and status, registered address etc.) and keep a duly updated register containing the list of shareholders as well as the number and category of shares held by each shareholder.



- **Beneficial ownership**

The process of gathering information on the beneficial ownership of legal entities is more complex. Beneficial ownership of a legal entity is identified through three main criteria. According to the first criterion the beneficial owner of the company is the natural person who may control the legal person through ownership interests, either through holding a certain percentage of the ownership interests (threshold approach) or through exercising de facto control over the entity, alone or together with other shareholders (majority interest approach).

The second criterion identifies beneficial ownership in the natural person(s) who controls the legal entity through other means. Other means include the natural person being personally connected to other natural persons who actually have control of the ownership of the legal entity; the natural person may also control the entity by financing it or by having family relationships with other persons in control.

The third criterion is a residual criterion used when no natural person is identified according to the other two criteria. The third criterion gives relevance to the natural persons exercising control of the entity through holding positions within the legal entity. The identified natural person is responsible for strategic decisions that fundamentally affect the business practices or exercises control over daily affairs through holding a senior management position.

The information on beneficial ownership should be recorded and available for consultation. Recommendation 24 establishes three mechanisms to ensure that the information is collected and available.

By adopting the first mechanism, countries require company registries to obtain this information and keep it up-to-date. An efficient company registry holding beneficial ownership information might contain: basic and beneficial ownership information

Increased transparency is definitely a common trend for the coming years

on the companies, annual updates of that information, declarations about the ownership structure, verification of the identity of beneficial owners, etc.

According to the second mechanism, companies should obtain and hold information on beneficial ownership. With regard to this aspect, shareholder lists contain information on legal ownership but not necessarily on beneficial ownership, therefore they might not be sufficient to comply with the obligation. The second mechanism requires companies to take reasonable measures to obtain the information on beneficial ownership.

Examples of reasonable measures to obtain the information are: restrictions upon shareholders who fail to provide beneficial ownership information, sanctions against shareholders who provide false beneficial ownership information etc.

The third mechanism relies on existing information contained in sources already existing: company registries, financial institutions and designated non-financial businesses or professions (including customer due diligence information), other companies and competent authorities.

Examples of other sources of information are: tax authorities, financial institutions subject to AML/CFT obligations, asset registries (land, property, shares) etc.

Regardless of the mechanism chosen, countries have an obligation of co-operation with authorities and they must appoint at least one person in the designated country to co-operate with authorities on behalf of the legal entity. Additionally, companies must maintain the information for at least five years.

Trusts are regulated in Luxembourg by the Law of 27 July 2003 which ratifies the Hague Convention of 1 July 1985 relating to the law applicable to trusts and their recognition

Enhancing transparency of legal arrangements – Recommendation 25

Legal arrangements are defined as *'trusts or other similar legal arrangements'* including fiducie, treuhand and fideicomiso. Trusts are usually established easily so that registration requirements are infrequent. Countries should identify ML/TF risks connected with trusts and similar entities, including risks related to jurisdiction or specific services provided by the legal arrangement.

Countries where national laws allow and recognise trusts should require trustees to obtain information on the beneficial ownership of the trusts and to keep that information up to date. Beneficial ownership information in a trust includes information on: the identity of the settlor, trustee protector (if any), beneficiary or class of beneficiaries or any natural person exercising ultimate control of the trust, as well as any information on regulated agents or service providers to the trust (e.g. advisers, managers, accountants etc.).

Countries whose national laws do not contain provisions on trusts or which do not recognise trust or similar legal arrangements are not exempt from obtaining information on beneficial ownership of trusts.

A trust may be constituted under and regulated by the law of one country but it can be administered in a different country. Therefore all countries should adopt measures that bind trustees to disclose their status to financial institutions or designated non-financial businesses or professions. Additionally, professional trustees should record the information for at least five years following their involvement with the trust. All countries should also arrange additional measures to facilitate access to information on the beneficial ownership of trusts. Several measures could serve the above-mentioned function. A registry of trusts could gather information on beneficial ownership, which would be available in a timely manner to competent authorities and for international co-operation.

Competent authorities, especially tax authorities, could be another important source of information on beneficial ownership; automatic exchange of information between authorities should facilitate the passing on of this information to competent authorities in foreign countries. According to Recommendation 22, designated non-financial businesses and professions are also subject to record-keeping obligations when dealing with legal arrangements. Specifically, trust and companies service providers are subject to record-keeping obligations when acting as a trustee of an express trust (or equivalent function for similar legal arrangements) and when acting as a nominee shareholder for another person.

Effects on Luxembourg

The first addressee of the implementation of the FATF Recommendations is the legislator. It is explicitly expected that the legislator should set up national provisions that will enable the country to comply with the Recommendations, both for legal persons and for legal arrangements.

The second class of addressees of the Recommendations consists of companies and legal entities in general. They have the obligation to comply with the provisions set out at the national level by the legislator.

Legal entities are expected to gather the information on beneficial ownership of the company and to keep it up to date in their records. Moreover, each legal entity must appoint one person in Luxembourg designated to co-operate with authorities upon request.

The third class of addressees of the Recommendations includes designated non-financial businesses and professions as well as trust or company service providers; their role is especially crucial in identifying and obtaining information on legal arrangements, particularly on trusts. Trusts are regulated in Luxembourg by the Law of 27 July 2003 which ratifies the Hague Convention of 1 July 1985 relating to the law applicable to trusts and their recognition.

The Grand Duchy of Luxembourg allows and recognises trusts and they are regulated according to the law chosen by the settlor. Regardless of the law chosen by the settlor, if the trust is administered in Luxembourg, beneficial ownership information should be available in Luxembourg as well. According to Recommendation 22 designated non-financial businesses and professions should be subject to record-keeping obligations. The latter provision needs to be considered in parallel with legal professional privilege and legal professional secrecy protected by the Law of 10 August 1991 on the Profession of Lawyer and by the Criminal Code.

Transparency is a common trend. Earlier in the year, Luxembourg passed the Law of 28 July 2014 on Immobilisation of Bearer Shares and Units. Formerly, holders of bearer shares were not required to be identified in the shareholders' register of companies. The OECD's Global Forum on Transparency and Exchange of information for tax purposes recommended that Luxembourg should take appropriate actions to ensure the availability of information relating to the holders of this type of shares in all circumstances. As a result of the Law, the depository must be a Luxembourg professional such as credit institutions, professionals in the financial sector, qualified lawyers and chartered accountants.



Readers are reminded that Deloitte Luxembourg does not engage in the provision of legal advice and any matter requiring such advice should be referred to professional legal advisers.



How to make financial crime prevention pay-off Implementation strategies to reap the benefits of the holistic model

Piero Molinario
Partner
Forensic & Dispute
Deloitte Italy



It is difficult to quantify the costs of financial crime—there is no doubt that it has become a significant issue for organisations and one that is more challenging by the day

Introduction

For over two hundred years, the world of academia has studied the relationship between economic business cycles and increases in crime.

Notwithstanding other aspects that may contribute to increases in criminal activity, the last economic recession has, undoubtedly as measured by the number of enforcement actions reported in the media, accelerated the quest to uncover criminal activity, ranging from fraud and corruption to money laundering and tax evasion.

In this respect, the recent economic crisis has been something of a turning point in the regulatory response to financial crime around the world. The failure of light-handed regulation and risk assessment by both the private sector and regulators has significantly changed the landscape in terms of expectations and ways and means to address them.

In this article, we discuss implementation strategies that, based on lessons learned, have enabled organisations to gain the benefits promised by the ever more prevalent consolidated approach to white-collar crime prevention.

The inescapable pressures of tackling financial crime

Arguably, legislators, regulatory bodies and enforcement authorities have long deputised the private sector in the global fight against financial crime. This is especially true for the financial service industry with respect to money laundering and terrorist financing but also for other industries with respect to corruption, bribery, fraud, tax evasion, insider trading and more. Over the years, the work of supranational standard setting bodies and of particularly rigorous legislators of countries such as the U.S., UK, Australia and more has created a fine-mesh net of international standards, laws with an extraterritorial reach and demanding domestic regulatory frameworks (e.g. FATF recommendations, USA PATRIOT Act, FCPA, UK Bribery Act, etc.) that have 'raised the bar' globally.

This evolution, characterised by an imperative to fight financial crime and the intense pressure brought about by governments' enforcement actions around the world, has increased the cost of doing business. In parallel, the private sector has increased its focus on risk management and thus, among other things, on proactively trying to weed out illegitimate and illicit activity to manage the risk and implications of non-compliance and to preserve reputation.

This convergence has created a very interesting environment where not only governments but also the private sector is concerned with financial crime prevention. Not surprisingly, the higher level of scrutiny

and expectations in relation to financial crime and risk management has become a stay-awake issue for corporate directors and senior management around the world, who are seeing an increased expectation, both internally and externally, for compliance programmes that are effective at addressing risk. Consequently, effective compliance has become central to achieving business strategy. While it is difficult to quantify the costs of financial crime—which can include direct losses, record-breaking fines for non-compliance, penal actions against individuals, lawsuits and reputational damage—there is no doubt that it has become a significant issue for organisations and one that is more challenging by the day.

Over the last decade, organisations have made significant investments to be compliant with anti-money laundering, anti-bribery and corruption and anti-tax evasion laws and regulations. In the beginning, many organisations were more reactive, often implementing policies, procedures and controls in response to regulatory requirements that were more prescriptive in nature. Generally, organisations were fighting financial crime in silos (e.g. with an AML department, a Fraud Investigation Unit, etc.), and within those, they were focusing on the compliance chores or processes stemming from the regulations (e.g. client onboarding, transaction monitoring and reporting, vendor screening). In a quest to manage their risk exposures more effectively while containing the ballooning cost of compliance, many organisations began to view financial crime in a more holistic way.



The case for moving from a fragmented to an integrated approach

As crimes continue to increase in subtlety and sophistication, and may appear to discrete detection processes and intelligence systems as a set of unconnected and potentially normal activities and behaviours, merging unconnected financial crime programmes is the only way that organisations can build an accurate defence mechanism.

Without an integrated approach, firms will likely continue to invest in activities that simply do not provide the flexibility to keep up with changes in the regulatory landscape or the increase in sophistication and creativity of the more nimble criminals. With no way of joining the dots in their data, the effectiveness of the risk management will eventually degrade.

Firms that fail to improve or at least maintain effective measures against financial crime are likely to suffer greater financial loss and reputational harm, and organisations and their employees will be left more vulnerable to punitive action by the regulators.

With a legacy of desperate approaches to contend with and increasing cost pressures, organisations could easily choose a path of minimal compliance. Before they take this line though, they should consider whether an integrated approach, centred on bringing their data and analytics together, would help improve the quality of their financial crime prevention efforts while simultaneously reducing costs.

Reaping the benefits of an integrated approach

A consolidated model to financial crime enables previously disconnected areas of financial crime prevention activity to be linked, in order to explore the overlaps, synergies and linkages that exist between cross-organisation processes and data sets. Said interconnections can then be used to build risk mitigating measures as well as models capable of estimating the probability of future crimes occurring, which means organisations can become proactive rather than reactive, and thereby reduce the potential for significant losses. Further, a centralised model allows managers to derive key performance indicators and timely and accurate management information, which can then be used for essential benchmarking and reporting, which in turn can increase quality and reduce cost.

Our Forensic partner Ivan Zasarsky at the Deloitte Australia office, provides us with insight on the benefits of a consolidated model: *'It seems that when alignment of managed interests become a priority, any number of unintended opportunities emerge. We have seen that when the adversaries (bad actors) conduct their operations ... clearly, they do not play within a business unit or specified jurisdiction. When protection of the institution is everyone's responsibility, the engagement of key departmental and line of business leaders is essential. In my experience, the alignment of enterprise-wide financial crime productivity results in: reduction of duplication / redundancy (e.g. processes, applications, data, etc.); increased transparency of risk (e.g. more effective identification, management, mitigation, etc.) and heightened mindshare (e.g. culture shifts, enhancement of front line awareness, corridors of communication within and outside of the organisation, etc).'*

How have organisations successfully transitioned from the pigeonholed approach so loved by the agile and flexible 'bad actors' which treated criminal activities as if they were separate and distinct (e.g. fraud from money laundering) to a consolidated view and approach to financial crime? It has not been without challenges, however, some have managed the transition and there are lessons to be learned. Following is an account of some key considerations that stem from our collective global and cross-functional experience.

Live by the findings of the enterprise-wide financial crime risk assessment

Rather than continuing to pump time and money into a patchwork of compliance chores and systems to tackle financial crime, organisations should start afresh, from an objective assessment of their risk profile. They should analyse, in detail and holistically, their exposure to financial crime risk. Doing so, with a methodical and repeatable approach, will not only identify, assess and quantify the present or eventual risk exposures (e.g. a subset of clients or services, a newly formed business or one expanding in a new market, a weaker procedure, etc.) but also the related mitigating measures currently in place (or not) in terms of policy, procedures, and controls. From the assessment of the risk exposures, mitigating measures and the resulting residual risk or 'gap' will stem an enterprise-wide risk assessment heat map that will serve as the starting point for the consolidated financial crime prevention strategy. From the latter, the organisation will then develop a target-operating model that aligns strategy, people, process, technology and data capabilities.

Set a resilient consolidated financial crime strategy

To effectively detect, assess, prevent and respond to financial crime, organisations need to design a strategy that takes a holistic view of financial crime risk as determined through the risk assessment findings and that is sufficiently agile. A static or reactive approach will likely fail, while a fragmented one is not enough. Institutions need to iterate their financial crime management strategy with the same commitment and effort as they would their corporate or customer strategy. They need to know where they are going to focus their efforts and how they will be successful in mitigating financial crime as a result of those efforts. Only then will it become clear that the fight is a joint effort that needs to be countered with common capabilities and systems.

Key aspects of resilient strategy often include:

- The overall organisation vision on how and why to combat financial crime
- The main pillars or themes for a consolidated fight against financial crime (leading rather than following the industry, risk assessment approach, tone from the top, leveraging all available data, etc.)
- Clear and measurable objectives that will need to be attained enterprise-wide in terms of efficiency, effectiveness and quality



Transition to a truly consolidated target operating model

Organisations have approached integrated financial crime risk management by assessing the current state for each crime area, enterprise-wide, creating a vision for where they would like to be, developing an outline of the target operating model and developing a roadmap (even if of three years or more) to help get from the current state to the future state.

Assessing the current state for each crime area, enterprise-wide often involves assessing the cost of financial crime risk management, by cost type, considering people, technology and data (including the costs to obtain, store and analyse it), the processes used to manage the data and control its quality, teams organisation and their responsibilities, performance in terms of how it is measured and reported, steps are taken to ensure regulatory compliance.

Creating the future state, often involves looking at the following questions:

- Are we actively seeking out opportunities to align areas of financial crime risk management?
- Who has overall responsibility for managing and fighting financial crime?
- Have we identified areas that can be more effectively aligned, for example, Know Your Customer (KYC) or Know Your Vendor (KYV) data definition (including static and transaction), technology, analytics, investigations, policy and procedures, supporting standards, governance (including functional teams and committees), management information, training development and delivery?

Developing the outline of an integrated target operating model should take into consideration the uniqueness of the organisation and again leverage the findings of the risk assessment.

The key areas of the operating model often address:

- **Strategy:** including financial crime risk definition, identification and assessment, and financial crime policies and frameworks
- **Operations and people:** including structure, skills, process alignment and optimisation, operational effectiveness and efficiency, and talent recruitment, development and training
- **External relations and reporting:** including reporting to the law enforcement authorities, regulatory bodies, industry bodies and contact with the media
- **Governance and compliance:** including compliance with and adherence to policies, assurance testing, periodic policy review, IT system governance, and incident and breach reporting
- **Data and its quality:** including a centralised data hub and data's fitness for purpose, data quality measures and monitoring, root-cause analysis of data quality issues and tools in use

A centralised approach also allows managers to derive key performance indicators, as well as timely and accurate management information, which can be used for essential benchmarking and reporting.

Finally, the exercise should determine how often the effectiveness of the framework should be reviewed and how often the organisation should look for further enhancements.

Developing a roadmap to transition from the current state to the future state will likely involve a set of prioritised initiatives and projects, a high-level implementation plan and a business case, addressing questions such as how 'effective' and 'efficient' approaches are defined and how 'quality' and 'success' are defined.



Leverage technology

It is clear that technology plays a critical part in combating financial crime. Technology tools can give an organisation a more holistic view of their data, highlight potential areas of risk and let it be more focused and targeted in its efforts to combat financial crime. While technology is essential, the design, build and execution of this technology must be aligned to the strategy. The technology question should only be answered after the strategy is set: is the technology yielding enterprise-wide results that meet the set efficiency, effectiveness and quality objectives?

Embrace analytics

The target operating model should be constructed around a central analytics hub, the firm's engine room for financial crime risk management, which delivers high quality, actionable insights that can be used to detect, prevent and deter crime. In existing environments, this is often achieved by building a data warehouse that feeds from legacy systems, with a longer-term plan to merge or replace those systems.

Analytics is an underutilised resource for dealing with bribery, money laundering and corruption, according to a new Deloitte survey. Tony DeSantis, principal at Deloitte Transactions and Business Analytics LLP in the data analytics practice, stated that financial crime detection and prevention efforts have often been ad hoc or disparate and not fully integrated in many organisations, and that EFM (enterprise fraud and misuse management) is a way to have a more holistic approach to managing financial crime detection. It can allow organisations to span multiple businesses, and international borders. According to DeSantis, many organisations are unsure of where to begin and how to effectively apply analytics and those out in front are honing early efforts on specific schemes or problematic regions by focused, risk-based approaches and methodologies.

The term 'analytics' describes a range of data-driven approaches that, when combined with deep business and sector knowledge, can highlight suspicious activity normally obscured by large data volumes or discrete data channels (data stovepipes). Ideally, the analysis draws on data sources from all over the organisation including operational activity and existing financial crime activity; and potentially from external sources, to establish insights that provide a comprehensive and accurate assessment of risk and is particularly powerful where the criminal activity is dispersed across several data sets.

As links are made between people, account activity and transactions, a wide variety of techniques exist, applied alone or in combination, to reinforce and score links to help analysts make connections and understand the overall risk.

In addition to the data and technology for analysis, the operating model focuses on linking previously disconnected areas of financial crime activity, to explore the overlaps, synergies and linkages that exist between cross-firm data sets. Analysis can focus on historical data, to detect previously unnoticed crimes, or use data flowing into the firm to generate alerts that trigger more in-depth analysis. Ultimately, the data can be used to build models capable of estimating the probability of future crimes occurring, which means firms can become proactive rather than reactive and thereby reduce the potential for significant losses.

As it is based on facts rather than hypotheses and therefore relies both on data volume and data quality, the analytics hub does not try to guess associations. In some cases, data volume can provide a remedy for situations where data has been corrupted either accidentally or through systemic error, or where data fields simply have not been completed.

The use of analytics is often compared to 'finding a needle in a haystack'. The unified approach to financial crime risk management is effective not only because the analytics ultimately finds more 'needles' but also because it very effectively characterises and removes the 'hay', leading to greater efficiency as well as a better understanding of the overall financial crime situation.

Advanced analytics will help companies predict and identify trends and patterns in financial crime risk that are not otherwise easily discernable. Overall, the emphasis must be on prevention and early detection, leveraging technology and analytics to proactively identify issues or potential issues before they turn into front-page news. Analytics based on real-time flows of consolidated enterprise-wide data and not pools of static data will be the key in the future as the data in organisation continues to increase. Analytics, particularly in the context of knowing the key actors (customer, vendor, employee, etc.) must be consistent and holistic across the organisation's businesses and departments. It is not only imperative from a financial crime management perspective but also from an efficiency perspective.

Analytics, particularly in the context of knowing the key actors (customer, vendor, employee, etc.) must be consistent and holistic across the organisation's businesses and departments

Back to basics

Mark Anley, a director at Deloitte South Africa, indicates that the most commonly used prevention mechanisms for mitigating financial crimes are segregation of duties and job rotation, while the most commonly used detection mechanism across the region is quality risk-based internal audits. Perceptive organisations have invested in the development of financial crime programmes that have thorough and detailed enterprise-wide policy requirements, consistent prevention principles embedded in the procedures and controls that have stood the test of time. Such programmes are aligned with the strategy and based on the results of the recurring risk assessment and most importantly contain the key, often basic elements that regulators, consultants and organisations have found to be most effective at preventing and detecting internal and external financial crimes.

These may include:

- External independent testing
- Internal audit testing that is tailored to the risk assessment findings
- Worst-case scenario testing based on actual most famous and/or most recent enforcement actions and media reported cases
- Financial crime type specific training with detailed case studies
- Examples of red flags and end-of-course quiz, testing of system effectiveness by consultants (transaction monitoring systems, sanctions filters, etc.)
- Thorough implementation and recurring testing of the segregation of duties, 'four-eye', 'fit for purpose' and job rotation principles applied to all the high-risk areas identified during the risk assessment

Adopting a proactive approach to testing can assist companies in actively preventing circumventions of their compliance programmes and is usually far more cost-effective than a reactive approach.

Non-compliance with regulatory requirements (both domestic and international) may result in significant financial loss and reputational risk across the jurisdictions in which an organisation operates.

Technology tools can give an organisation a more holistic view of their data, highlight potential areas of risk and let it be more focused and targeted in its efforts to combat financial crime

Change the culture

Failure to prevent or detect issues is often not because the programmes or controls themselves are lacking. More often, it is a failure of culture and a lack of effective change management. For example, senior leaders may not be setting a strong or consistent 'tone at the top' about acceptable and unacceptable behaviours.

This often manifests through fiscal or scope constraints on financial crime projects, dictating an unsustainable bare minimum approach. Alternatively, there simply is not enough attention by all key stakeholders across the entire institution to adopt and execute on the new policies or processes.

Experience tells us that staff training and awareness efforts are often under-resourced. The infrastructure to prevent financial crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time—culture is what enables and drives those appropriate behaviours.

Accomplishing this transition typically involves a focused change management effort for the organisation. Executives and directors of financial services companies can no longer support a 'bare minimum' approach to compliance; it is just too risky for the corporation and personally. Corporate collapses and regulatory actions have proven 'bare minimum' approaches have and will certainly fail in the future. Organisations are simply too exposed as they now collect and have access to all the information they require to mitigate financial crime risk proactively.

Executive teams and senior management need to find ways to demonstrate a commitment to financial crime compliance. In addition to setting the appropriate financial crime strategy and communication plan, organisations will often consider making compliance a component of the performance evaluation process to clearly define the compliance responsibilities of management in the different lines of business and departments.

Conclusion

The recent economic crisis has been something of a turning point in the regulatory response to financial crime around the world. An imperative to fight financial crime accompanied by an intense pressure brought about by governments' enforcement actions around the world, has increased the cost of doing business at a time when the private sector was already increasing its focus on risk management. Not surprisingly, the higher level of scrutiny and expectations in relation to financial crime and risk management has become a stay-awake issue for corporate directors and senior management around the world. While it is difficult to quantify the costs of financial crime, there is no doubt that it has become a significant issue for organisations and one that has resulted in significant investments to be compliant with anti-money laundering, anti-bribery and corruption and anti-tax evasion laws and regulations. In a quest to manage their risk exposures more effectively while containing the ballooning cost of compliance, many organisations began to adopt a holistic view to financial crime.

Organisations have successfully transitioned from the pigeonholed approach so loved by agile and flexible 'bad actors' to a consolidated approach to financial crime but not without challenges. In this article, we have provided an account of some key considerations that stem from Deloitte's collective global and cross-functional experience, which include: living by the findings of an enterprise-wide financial crime risk assessment so that it can serve as the starting point for a consolidated financial crime prevention strategy that is resilient. From the latter, transition to a target-operating model of governance, people, process, and controls that is aligned with the strategy and that leverages technology and embraces analytics, without forgetting the basics of effective compliance. Still, failure to prevent or detect issues will result even in the best consolidated financial crime programmes and controls in place if a culture of compliance is lacking. Ultimately, this can only be addressed by senior leaders' setting a strong and consistent 'tone at the top'.



Positioning the internal audit function within the Solvency II framework

Key challenges

Jérôme Sosnowski
Director
Governance, Risk
& Compliance
Deloitte Luxembourg

Ludovic Bardon
Senior Manager
Audit
Deloitte Luxembourg

Deborah Guez
Manager
Governance, Risk
& Compliance
Deloitte Luxembourg



Throughout its fundamental review of the capital adequacy regime of the European (re)insurance industry –*Directive 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance as amended ('Solvency II' or 'the Directive')*, entering into force on 1 January 2016—will introduce revised risk management and governance standards.

These revised standards will cause the system of governance of (re)insurance organisations to evolve with the implementation of mandatory key functions, adequate articulation of which is crucial to provide for sound and prudent management of the business.

Of the key functions enforced by Solvency II, the internal audit function intends to remain entirely responsible for the examination and evaluation of the adequate functioning and effectiveness of internal control systems and all other elements of the system

of governance, along with the evaluation of whether such internal control system remains sufficient and appropriate for the organisation's business.

While it is expected that the role and objectives of the internal audit function will not deviate from its primary focus in the Solvency II framework (an assurance activity for those charged with governance of the organisation, designed to add value and improve operations), some key principles are to be properly followed during the implementation.

Major challenges for the internal audit function under the Solvency II regime

Key features of the internal audit function

The internal audit function is defined as an independent, objective assurance and consulting activity whose role is to add value, improve an organisation's operations and ensure the respect of regulatory obligations. It helps an undertaking to accomplish its objectives by providing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, the actuarial function, the compliance function and internal governance processes.

The internal audit function can also be seen as a tool for improving an undertaking's operations and related controls by providing insight and recommendations. It provides value to governing bodies and senior management as an objective source of independent advice.

However, beyond this generic definition of the internal audit function, key features have to be respected in order to ensure an appropriate working of the function within the framework of Solvency II and in compliance with Institute of Internal Auditing (IIA) standards.

These key features are the following:

1. Independence and objectivity

In order to comply with Solvency II and IIA standards, the internal audit function will have at all times to be independent of the activities it audits. Such independence will allow the internal audit function to perform its work freely and objectively. It will also allow the function to render impartial and unbiased judgments essential to the proper conduct of its activities objectively.

Indeed, the independence of the internal audit function is incompatible with the situation in which:

- The staff of the internal audit function is in charge of tasks it is called upon to check or tasks which are not related to its area of control
- The internal audit function is, from an organisational point of view, included within the business units it controls or reports hierarchically to them

The authority that the internal audit function must have also requires that it should be able to exercise its responsibilities, on its own initiative, express itself freely and access all external and internal data and information (in all business units of the institution it checks) deemed necessary to fulfil its role.

The authority of the internal audit function must be objective in carrying out its work.

Even if, in many situations, this can be challenging, the internal audit function must exercise independent thought and judgement. The head of the function should not make his/her own judgment conditional upon that of other persons including, in particular, those checked.

Objectivity also requires that conflicts of interest are avoided. To achieve this, the internal audit function must remain free from interference by any element in the organisation, including in matters of audit selection, scope, procedures, frequency, timing or report content, to enable the maintenance of the necessary independent and objective mental attitude. Internal auditors should also have no direct operational responsibility or authority over any of the activities audited.

Accordingly, they will not implement internal checks, develop procedures, implement systems, prepare records or engage in any other activity that might impair their judgement. In order not to challenge their independence of judgement, the persons responsible for internal audit cannot be in charge of the preparation or establishment of elements of the administrative organisation and internal governance. However, this fundamental principle does not prevent them from taking part in the implementation of a sound internal control mechanism through observations and recommendations that they provide in this respect.

In all cases, internal auditors must exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. They must make a balanced assessment of all relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

The co-operation of the internal audit function with other governance functions is also expected to increase through improved exchange of information

2. Proficiency and due professional care

In parallel, all internal audit engagements must be performed with proficiency and due professional care. This means that internal auditors must have or must acquire, where necessary, the knowledge, skills and any other competences needed to perform their individual responsibilities.

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. However, due professional care does not imply infallibility and, in some cases, the internal audit function should legitimately consider the support of an external expert in the subject, in order to ensure an adequate level of expertise on specific areas to be covered according to the internal audit plan.

In order to achieve reasonable proficiency and due professional care, it is thus important that internal auditors enhance their knowledge, skills and any other competences whenever possible through continuing professional development.

3. Professional ethics

In order to comply with professional ethics, the internal audit function must adhere to the IIA's mandatory guidance including the IIA's Definition of Internal Auditing, Code of Ethics and its Standards. This mandatory guidance constitutes the principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit function's performance.

Of course, the internal audit function must also adhere to relevant policies and procedures of the company covering the professional behaviour and ethics of the undertaking's employees.

4. The internal audit charter

All these key features will have to be described in the internal audit charter which is the cornerstone defining the purpose, authority and responsibilities of the internal audit function. This document must in all cases be consistent with the the IIA's Definition of Internal Auditing, Code of Ethics and its Standards.

The internal audit charter, which is drawn up by the internal audit function, will have to be approved by both the executive board and the board of directors of the company. Its content is to be brought to the attention of all staff members of the company, including those who may work in branches and subsidiaries.



How the internal audit function will contribute to an effective system of governance

In addition to the set-up of an internal audit function, the Solvency II framework Directive requires insurance undertakings to have an effective system of internal governance in place. Its objective will be to provide *'a sound and prudent management of business'*, in which the position of the internal audit function has been emphasised.

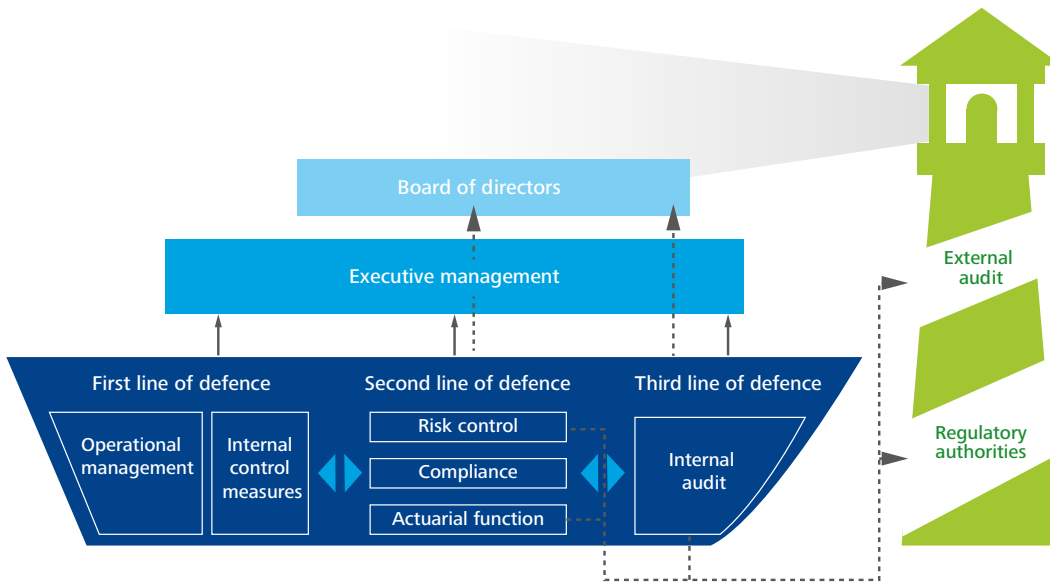
Indeed, the governance system of Solvency II implies four key functions, namely the risk management, the compliance, the actuarial and the internal audit functions.

This model requires responsibility to be differentiated and distributed at three different levels named lines of defence:

- 1 The first line of defence consists of the business units that take or assume risks within a pre-defined policy and limits and carry out checks.
The types of checks performed consist of:

 - Daily operational checks
 - Critical on-going checks: persons in charge of validation
 - Checks performed by the authorised management on matters for which they are directly responsible
- 2 The second line of defence contributes to the independent risk control. The challenge of the second line of defence functions is to ensure compliance with and execution of risk, actuarial and compliance strategies, approaches, and related management information.
- 3 The third line of defence is composed of the internal audit function. It provides an independent, objective and critical review of the first two lines of defence. As already detailed above, the objective of the internal audit function will be to provide an independent, objective and critical assessment of the design and effectiveness of the overall system of internal control.

Figure 1: The three lines of defence model



This model illustrated in the above figure puts in evidence where the separate functions operate within the governance structure of the insurance undertaking even though interactions/channels of communications must exist in order to avoid each line of defence operating within its own 'silo'.

Such a governance model, reflecting the regulatory expectation detailed in the *'Consultation Paper on the proposal for Guidelines on system of governance and own risks and solvency assessment'* (publication EIOPA-CP-14/017) points out the most critical challenges that the internal audit function of an insurance undertaking will have to achieve:

1. To impose itself in organisations where, until now, an internal audit function was not a regulatory obligation for (re)insurance undertakings in all EU countries. This objective will be achieved by clear communication of the role and responsibilities of the function within the organisation (i.e. an internal audit charter) as well as its operating procedure (i.e. internal audit plan, assignments, reporting and follow-up of recommendations).
2. To develop co-operation with other lines of defence while remaining independent and objective when performing internal audit assignments.
3. To have an extensive level of proficiency in order to be in a position, on the one hand, to issue recommendations relevant for the improvement of operations but also, on the other hand, to be considered within the organisation as being in a position to provide advice upon request from executive management or other governance bodies.

In this way, the internal audit function will appear a key part of this governance system and contribute to the soundness and prudence of an insurance undertaking. In this context, the internal audit function will have to extend its scope of intervention in covering this new governance framework more specifically.

Extensive role of the internal audit function within the Solvency II framework

Article 47 of the Directive requires (re)insurance organisations to provide for an effective internal audit function. The internal audit function must include an evaluation of the adequacy and effectiveness of the internal control system and other elements of the system of governance.

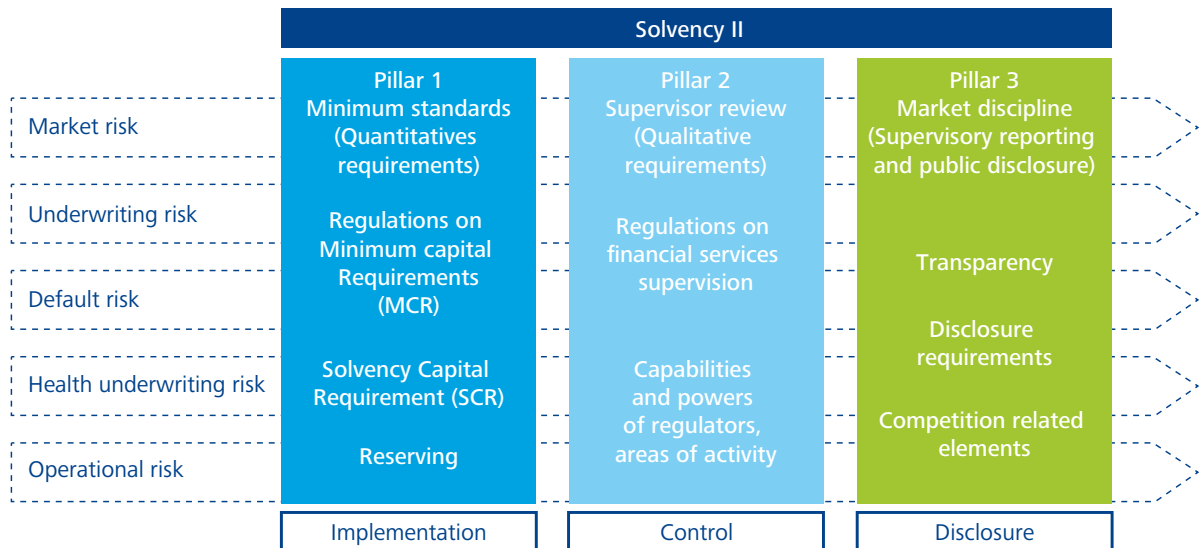
While the Directive states that the system of governance should be proportionate to the nature, scale and complexity of the operations of the organisation, it assumes, however, that the internal audit function must be in place and operate effectively, primarily in the reporting of any findings and recommendations to those charged with governance of the organisation.

Assuming the internal audit function operates effectively means that the internal audit function is expected to design and implement an audit plan that encompasses the whole internal audit scope (activities, components and functions) as amended by the Solvency II framework.

A comprehensive audit approach that should consider the whole spectrum of the regulatory requirements with the deployment of an integrated audit plan

The internal audit function has to consider all the requirements of the Solvency II framework, leading to an enlargement of the scope of internal audit and an impact on the audit approach and working programmes, since Solvency II compliance items are expected to be included in the carrying out of each internal audit assignment.

Figure 2:



As part of the extension of internal audit tasks prescribed by Solvency II, the review of the Own Risk and Solvency Assessment (ORSA) and Pillar 3 communication processes and outcomes can be highlighted:

1. Defined as *'the entirety of the processes and procedures employed to identify, assess, monitor, manage, and report the short and long term risks a (re)insurance undertaking faces or may face and to determine the own funds necessary to ensure that the undertaking's overall solvency needs are met at all times'*, the ORSA sheds light on the impact of strategic decisions on the organisation's overall solvency and its outcome. A yearly report submitted to the regulatory authority is subject to an independent review from the internal audit.

This review will be carried out to ensure that the ORSA process and outcome are appropriately designed and implemented, considering the following objectives as part of the internal audit approach: effectiveness of the ORSA governance and process, compliance with Solvency II requirements and timeliness of reporting, appropriateness of the risk models applied and consistency with the overall risk profile of the organisation and reliability and traceability of information supporting risk assessment.

2. Pillar 3 reporting and disclosures will also widen the scope of internal audit with the review of the processes in place supporting the preparation of both quantitative and qualitative information contained in the Solvency and Financial Condition Report (SFCR) and the Regulatory Supervisory Report (RSR). This review will aim at ensuring that this information is relevant, reliable, accessible and complete in all material aspects, consistent with the Solvency II requirements.

In the meantime, this expansion of the internal audit scope may also give rise to further collaboration between the internal audit function and the external auditor of the organisation. Indeed, it is expected that these reporting requirements will be subject to external audit, and, in some instances, the external auditor may decide to rely on the work performed by the internal audit function.

Within the organisation, the co-operation of the internal audit function with other governance functions is also expected to increase through improved exchange of information.



A fundamental role in the assessment of the internal control and governance systems

Within the three lines of defence model, the internal audit function provides assurance on the design and effectiveness of the overall system of internal control, including risk management and compliance functions.

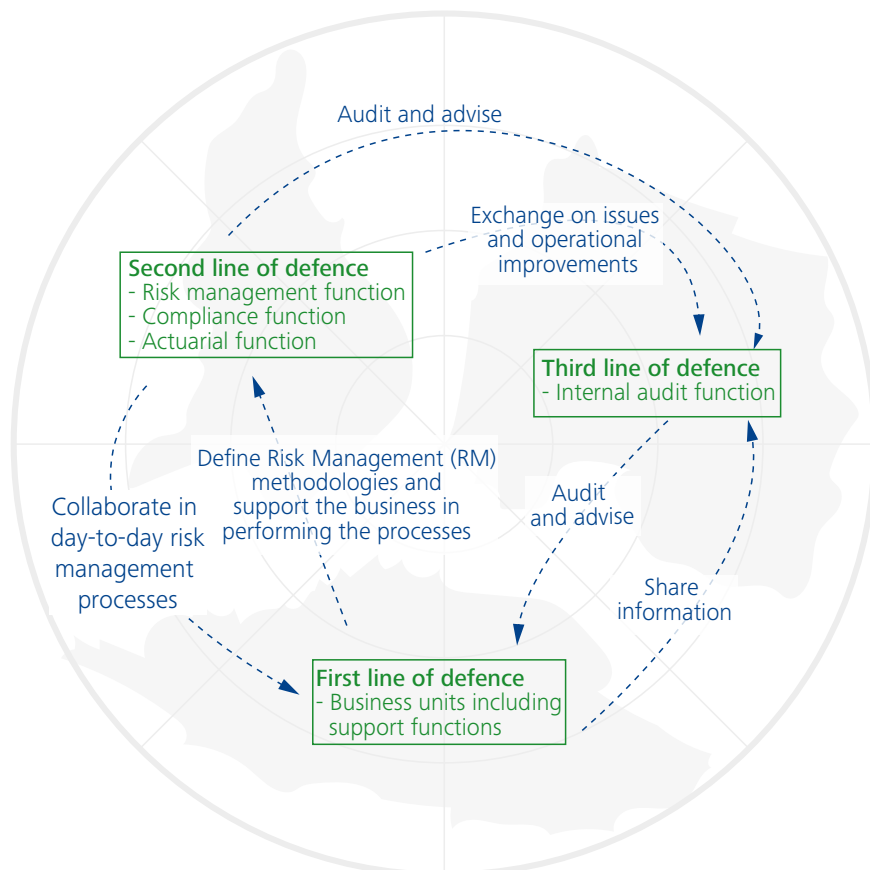
Despite having adopted the 'three lines of defence' risk governance model, some organisations still struggle to articulate how oversight is assigned among the governance functions and other support functions.

Transparent and fair apportionment of responsibilities for supervision is crucial to achieving an adequate organisational structure along with an appropriate segregation of responsibilities.

As the third line of defence, the internal audit function is uniquely positioned:

- To provide an independent assessment of the governance system
- To enhance the communication process between the different functions
- To foster the use of a common language throughout risk identification, categorisation and reporting processes

Figure 3:



Independent assessment of the governance system by the internal audit function relates in particular to assessing risk management and compliance functions.

- The monitoring of compliance with laws and regulations, including how the compliance function fulfils its responsibilities

Assuming that the internal audit function has the appropriate capability regarding matters of risk and regulatory interest, the audit scope should be focused respectively on:

Along with a broader scope of internal audit, the internal audit function is dealing with more diversified areas of expertise such as actuarial, regulatory and information technology matters.

- The effectiveness and efficiency of risk management systems in the context of both current and potential future risks
- In this context, risk management systems set out the necessity to review the adequacy of processes for identifying, measuring, assessing and reporting on all the risks resulting from the organisation's activities as well as the integrity and robustness of the risk management information systems, including the reliability and completeness of the data used

Consequently, internal auditors will have to broaden their technical skills continuously to ensure suitable competencies are available to achieve an independent and timely review of the internal control and governance systems.

Conclusion

The new governance system defined by Solvency II enforces the deployment of key functions and foresees that the internal audit function will play a fundamental role in the recurrent maintenance and assessment of internal control, risk management and governance systems and processes. This strengthened role becomes even more evident when the magnitude of the scope of audit is considered.

Beyond the existing guidelines and professional standards that are to be followed by the internal audit function, some major challenges appear when it comes to an effective implementation of the function: adequate professional knowledge and industry expertise are pre-requisites that entail investment in human capital and dedicated training in most organisations.

In that respect, the organisation could address this governance requirement by:

- The development of an internal audit department within the organisation, under the responsibility of a Chief Internal Auditor with strong knowledge of the industry and of internal audit standards and market practices
- Or the outsourcing of the internal audit function, with the use of external expertise that should be assimilated by the organisation, which will ultimately retain the overall responsibility for maintaining an effective internal control function



Risk appetite and assurance

Do you know your limits?

Paul Day
Partner
Banking & Capital Markets
Deloitte UK

Tim Thompson
Partner
Quantitative Risk & Finance
Deloitte UK

Stephen Boyd
Senior Manager
Risk & Regulation
Deloitte UK

Effective risk appetite

The need for an effective risk appetite framework was reinforced through observations of failures in its absence during the financial crisis. Global guidance has focused on delivering *'greater clarity and an elevated level of consistency among national authorities'*. It is therefore helpful to establish a common language within and between organisations and regulators when discussing this subject.

Design

An effective risk appetite framework combines a series of appetite statements, limits, measures and standards that together enable the board and the business to set, monitor and manage:

- Risk appetite
- Risk capacity
- Risk profile
- Risk appetite limit
- Risk appetite triggers

Effective design of a risk appetite framework demands a clear understanding of the relationships between these concepts, expressed graphically in *Figure 1*.

Figure 1: Interaction of Risk Appetite Concepts

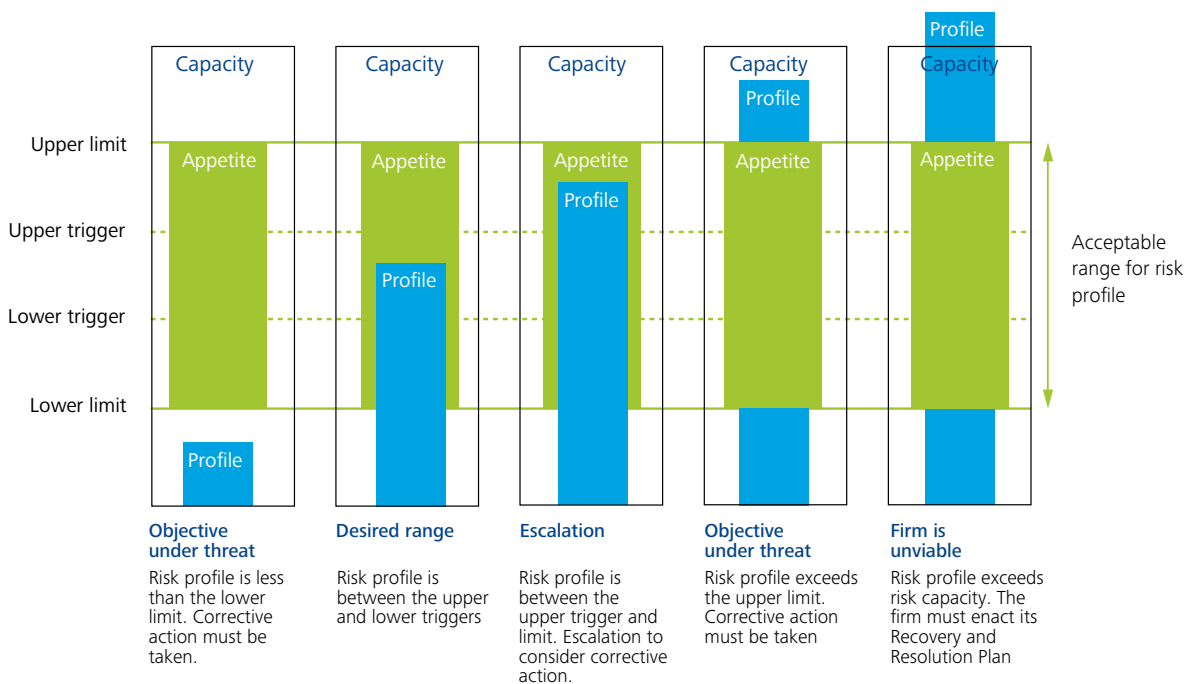
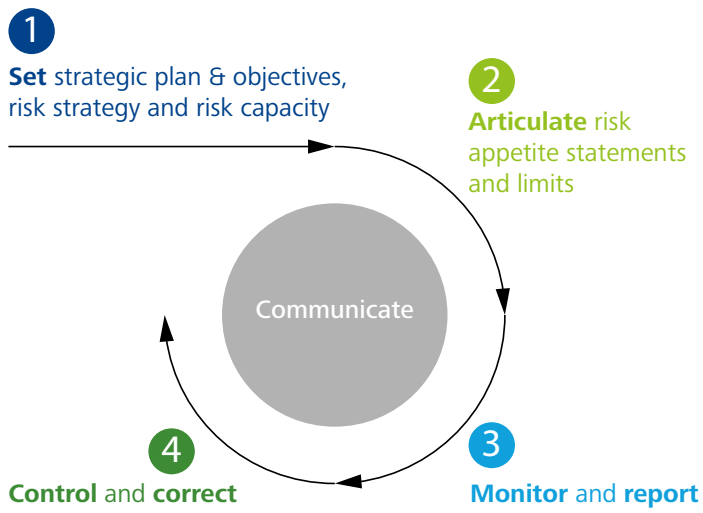


Figure 2: Risk Appetite cycle



Implementation

There should be policies and processes in place to:

- Set the risk strategy and objectives and ensure alignment to the strategic plan
- Determine risk capacity
- Set, articulate and cascade risk appetite statements and associated limits
- Monitor and report risk profile versus appetite and triggers
- Manage the risk profile

This should be a dynamic process, as depicted in *Figure 2*, with appetite and limits responding to the business environment and/or changes to risk capacity as required. Achieving this dynamism, and the breadth and depth discussed earlier, is greatly assisted by the use of a common organisational language with respect to the components of the framework.



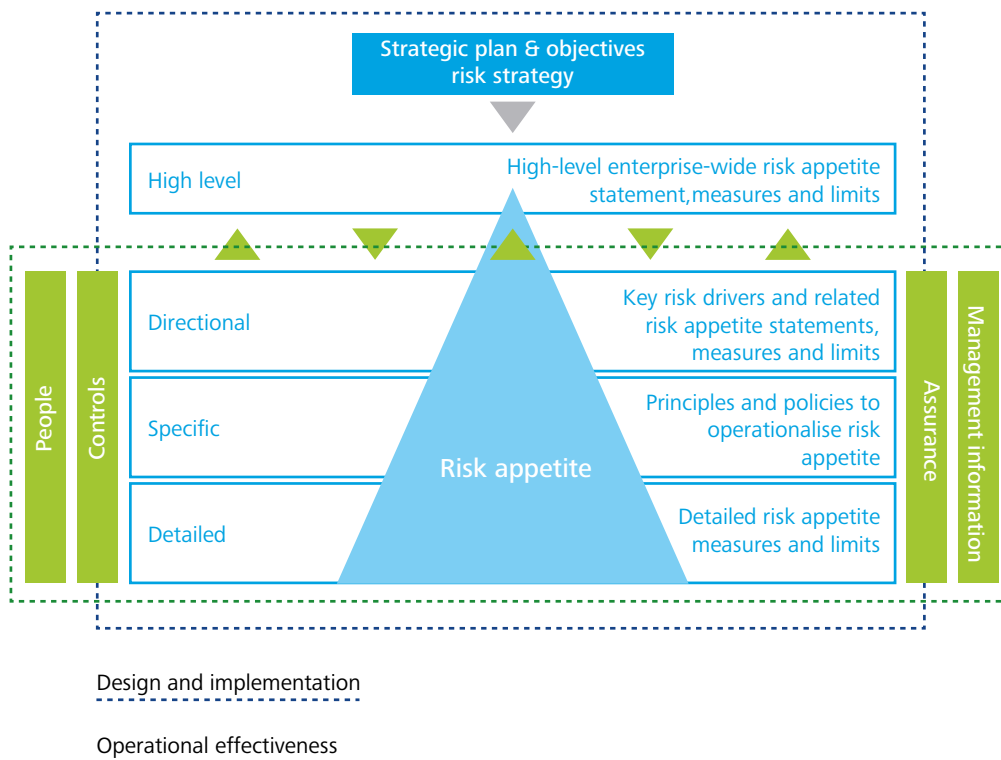
Considerations for internal audit

Internal Audit must deliver assurance on both the design of the risk appetite framework and its operating effectiveness. A properly functioning risk appetite framework contains key components at all levels of the business, and business level activity is not solely operationalising of board level risk appetite activity. Internal Audit should therefore ensure it carries out appropriate testing in all parts of the business.

Operational effectiveness

- **Risk measures** - Ensuring risk measures are complete and catalogued in risk registers and that linkage to risk appetite is apparent
- **Policy and framework** - Setting standards and assessing compliance with these standards. Risk appetite should be a consideration in all policy creation and management to ensure business practices are guided not only by strategic and operational constraints, but also within the constraints of risk appetite. It also ensures that as procedures and processes are developed to support policy, businesses are able to easily identify if activity would breach or impact appetite

- **Management information** - Internal Audit may review the way decision makers are presented with risk appetite management information, and question the prominence, aggregation and timeliness of measures and reporting
- **Assurance** - How is the appetite considered within assurance functions? Are the first or second lines providing assurance on areas which are not part of risk appetite? If so, what value does this add? Or crucially, are they reviewing areas which are not reflected in risk appetite? These factors point to a lack of embedding
- **Culture and embedding** - Internal Audit should be aware of any activity within the business which would illustrate how well risk appetite understanding and management is embedded within the business. This is evident by the acknowledgement of appetite, or the impact activity may have on appetite, through key decision-making such as new product approval processes or operational changes



Internal Audit must deliver assurance on both the design of the risk appetite framework and its operating effectiveness

Design and implementation

- **Strategy** - Internal Audit should assess the extent to which risk appetite statements within the firm align to the strategic mission statements of the business. Overall, strategy and appetite must reconcile. The risk appetite framework should support and inform business performance
- **Scope and qualitative measures** - These should assess whether risk appetite is considered for the entire risk universe of the business and evaluate how the framework incorporates and articulates non-quantitative risk exposures such as conduct and ethical or reputational risks. An effective risk appetite framework should be able to articulate and aggregate appetite measures across all risk types that the business is exposed to
- **Ownership** - The second line should provide the framework, tools and standards for risk appetite to be managed. The first line should set the risk appetite and make decisions surrounding it. Internal audit should seek to establish how clearly defined these responsibilities are

• Governance and management information -

Remediation plans should be clear and consistent to ensure appetite aggregation is accurate and appropriate, and tracked accordingly within risk governance. There should be clear delegated authorities and transparency to ensure accountability for decisions. Triggers should be appropriately managed with amendments controlled

Management information should be appropriately aggregated and escalated, with a clear line between appetite statements and detailed measures and limits. Any limitations should be appropriately acknowledged and disclosed upon each presentation to ensure informed decisions.



Conclusion

- Boards need to prioritise the quality and effectiveness of risk appetite frameworks as they will be subject to regulatory scrutiny.
- Internal audit should move to deliver assurance to the board on the control framework by reference to a firm's ability to manage activity within risk appetite limits.
- Internal audit actions should seek to drive a comprehensive and fully embedded risk appetite framework so that internal audit functions can then adjust their broader assurance plans based on the intelligence provided by framework monitoring, thereby maximising assurance effectiveness.
- Risk appetite is still evolving and, for some firms, is a complex topic. Internal audit functions should consider any limitations in terms of resources and ability when developing their approach to both assessing and utilising their organisation's risk appetite framework.





Managing social media risks to reputation risk

A hot topic on the board agenda

Henry Ristuccia
Global Governance, Regulatory
& Risk Strategies leader
Deloitte Touche Tohmatsu Limited

Michael Rossen
Director
Global Center for Corporate
Governance
Deloitte Touche Tohmatsu Limited

Social media sites are more than just venues for chatting about politics, travel, and family. They are an ever-evolving source of valuable information on customer and third-party views with a special focus on their attitudes, experiences and opinions.

At the same time, social media is a probable source for reputation risks, such as brand/reputation damage, legal and regulatory compliance, security and privacy, and employee/HR issues.

Savvy board leaders are taking note. They are helping guide social media strategy to enable people inside and outside the organisation to connect, interact, and share information in new and more efficient ways, from recruiting and talent management to facilitating product development and enhancing supply-chain performance. Today, social media touches everyone, with a host of uses across nearly all functions in an organisation. Not only are board directors keeping a watchful eye on the impacts of social media on the organisation – they are also becoming participants.

An understanding

With reputation risk being a top-level issue - and social media a domain for building or destroying reputations - board members are starting to ask more questions. These questions are leading to a deeper understanding of how these channels can affect reputation and the bottom line. A recent survey¹ conducted by Forbes Insights on behalf of Deloitte Touche Tohmatsu Limited (DTTL) revealed that 88% of more than 300 executives, mostly senior executives and board directors, were focusing explicitly on reputation risk as a key business challenge.

Moreover, companies attribute about 25% of their market value to reputation, according to a study presented by World Economics². It comes as no surprise that leaders are continuing to guide their organisations toward processes, tools, and talent that can help them prepare and respond to reputation challenges in the social realm today and well into the future.

¹ 'Reputation@Risk' (DTTL, October 2014)

² Simon Cole, 'The Impact of Reputation on Stock Market Value' (World Economics, February 2013)
http://www.world-economics-journal.com/Papers/The%20Impact%20of%20Reputation%20on%20Stock%20Market%20Value_3d2cbd00-f485-4dfe-b9bb-76b22c0c64ef.paper

An evolution

New reputation risks and old reputation risks are morphing in the social sphere, creating a perpetual state of evolving risks. Vocal, dissatisfied customers have always been a threat to reputation. Now they can project their dissatisfaction instantly across the globe via social platforms. This new model continues to evolve as individuals discover new sharing techniques, as the social media tools themselves advance, and as new information search/discovery tools give members of the public fresh ways to find content that might influence their perception of companies.

To capitalise on the opportunities presented by the use of social media, while also managing risks appropriately, boards need to evolve with this fast-moving and complex environment.

Aiding them in the evolution are new techniques, new technologies, and new tools that can help guide their organisations in addressing social media risk as part of reputation risk. Social media will remain a strategic territory where things move fast. A threat to reputation can move fast and grow fast. Board members need to make sure their organisations can move fast, too.

A single complaint on an issue is one thing, one hundred complaints on the issue can signal a trend and magnify the impact of reputational risk

Tools to address the challenge

Social media involves all organisations operating today, whether they are active participants in social media or not, and it comes with inherent risks that involve reputation. As noted above, those challenges may involve brand damage, legal and regulatory compliance, security and privacy threats, and employee/HR issues.

Beyond those risk areas, there is also strategic risk involved in social media. A social media strategy that does not line up with the organisation's overall strategic goals ultimately can create internal and external confusion. Failing to participate in the social realm can mean your organisation gets left behind as competitors tap the power of social media.

Getting perspective on reputation risk in the social world is an ongoing process. As board leaders continue to address social risk as one facet of reputation risk, they will see many conventional reputation risk problems reflected back at them. It is important to understand the new tools and techniques their organisations will need to bring to bear to address the challenges. Here are some key approaches that boards can consider to encourage their organisations to take to address evolving reputation issues in the social sphere.

- **Adopt a preemptive mindset when it comes to reputation risk**

Leadership should advocate a forward-looking approach, endeavoring to know where to look for problems, how to analyse them, and how to move forward addressing and mitigating any potential risks. Receiving and analysing complaints is one facet of managing social media risk. Organisations need to know not only how they will interact with those who complain (the remedies and the responses via social media); they need to be on the search for complaints in the early stages. A single complaint on an issue is one thing. One hundred complaints on the issue can signal a trend and magnify the impact of reputational risk.

New offerings, such as social-listening tools and analytics solutions, can help organisations sift through the social noise to identify a pattern of complaints before it evolves into a crisis. Monitoring, analysing, and pre-empting problems such as complaints can also provide organisations with intelligence they can use to design product improvements, develop new offerings, and expand into new markets.

- **Develop robust capabilities to monitor and manage reputation risk**

Creating a holistic view of current and potential risks is imperative. That view begins with discovery and with understanding who your stakeholders are so that you can develop plans to monitor and manage your interactions with them. Know that your organisation most likely has more than one face when it comes to social media. Understand that your audiences are more than readers of your high-level social media feeds.

Many people use social media as a means to contact or connect with a company. It is therefore important to read what customers are saying, the questions asked, any requests/suggestions made and overall feedback received. By doing so, companies can better equip themselves to make business decisions that address customer needs.

Organisations, however, must remember the need to build reputation, and monitor and manage reputation risk, among audiences besides a core customer base or the general public. They must consider the ways in which they connect with suppliers, with other companies in their industry, with employees, with potential employees and with regulators.

- **Manage reputation risk proactively**

Your organisation should know in advance how it will respond when threats to reputation emerge in the social sphere, whether the threat is a fraudulent social media page masquerading as official or whether the threat is a string of complaints garnering the attention of traditional media. If you wait until a major reputation-risk event happens, it will be too late.

Organisations must do more than actively police social media for reputation-risk problems. They should actively develop plans for identifying and responding to significant reputation-risk events as well as assign the roles and responsibilities for avoiding a full-blown crisis and for managing a crisis. Organisations furthermore need to deploy the right tools - for risk monitoring, for event simulation, for response and for communication - to ensure that they can act rapidly.



A threat to reputation can move fast and grow fast, board members need to make sure their organisations can move fast, too



More tools for the social toolbox

Beyond strategy and planning from the top, there are additional tactics and technologies that offer organisations tools to address long-term reputation challenges on the social front. Understanding these tools, and the potential investments required, can help organisations prepare for known and unknown social threats.

Data analytics and 'social listening' tools can help provide boards with real-time information on what their organisation is saying and what is being said about it, a capability that can help organisations create an 'early warning system' for reputation risks related to social media. Over the longer term, the tools can help identify patterns that can offer deeper insight into how a company's reputation is growing or faltering on social media.

Enterprise social platforms can give organisations a virtual place for sharing ideas and leading practices internally, including ideas for addressing social media related risks created on external social platforms. It is a 'fight fire with fire' approach using a social tool to address a social challenge.

An awareness of regulatory issues that touch on social activities can help position an organisation toward compliance and away from legal snags that can damage reputation. Various regulatory agencies offer guidelines on social media, and it is important for companies to understand and address the guidelines in their compliance efforts.

For example, the US Financial Industry Regulatory Authority (FINRA) has extensive guidelines concerning communications with customers via social media, blog participation, and advertising. Failure to adequately address compliance risks can expose an organisation to enforcement actions or civil lawsuits (which themselves carry reputational and financial risk). Blending a social-business governance strategy with risk management and compliance programmes can help organisations stay focused on this front.

Socialisation realisation

Understanding that reputation risk has transcended the conventional business realm and is evolving in the social realm is critical for organisational leaders. Board members know that it is not enough for executive leaders to understand the challenges. Nevertheless, understanding the challenges is the first important step, because they help set the tone and the direction for the entire organisation.

Increasingly, the fate of organisations depends on how well they present themselves in the online world and increasingly, that presentation occurs via social channels. Reputation risk is real, with very real consequences, and the social world is where the real action is happening.

Board members, working with other leaders, can help ensure that their organisations have a strategy for identifying and responding to reputation risk factors, and for knowing who is in charge of which social and reputation activities within the organisation.

Board members have an additional role to play. They are also social media participants and they realise that their online social interactions can have reputation implications, too. As participants, they have an excellent opportunity to conduct their own research in social media, exploring the space to find out what is being said about their organisations and are able to develop their own personal perspectives on reputation and reputation risk.

Contacts

CEO & CFO services



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



Ruth Bültmann
Partner - Strategy & Corporate Finance
+352 451 452 115
rbueltmann@deloitte.lu



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



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



Pierre Masset
Partner - Strategy & Corporate Finance
+352 451 452 756
pmasset@deloitte.lu



Simon Ramos
Partner - Strategy & Corporate Finance
+352 451 452 702
siramoss@deloitte.lu

COO & CHRO services



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



Pascal Eber
Partner - Operations Excellence & Human Capital
+352 451 452 649
peber@deloitte.lu



Filip Gilbert
Partner - Operations Excellence & Human Capital
+352 451 452 743
fgilbert@deloitte.lu



Bertrand Klein
Partner - Operations Excellence & Human Capital
+352 451 452 289
beklein@deloitte.lu

CIO services



Joël Vanoverschelde
Partner - Technology & Enterprise Applications Leader
+352 451 452 850
jvanoverschelde@deloitte.lu



Marc Halmes
Partner - Technology & Enterprise Applications
+352 451 453 710
mhalmes@deloitte.lu



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

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 & Hedge Funds Leader
+352 451 452 489
jyiplanyan@deloitte.lu

Technology, media and Telecommunications - Public Sector



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

PSF



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

Private Equity - Real Estate



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

Please do not hesitate to
contact your relevant experts
in the magazine

Contacts

CCO/CISO/CRO/CIA/BOD services



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



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



Eric Collard
Partner - Forensic, AML & Restructuring
+352 451 454 985
ecollard@deloitte.lu



Thierry Flamand
Partner - Insurance & Benefits Actuarial Advisory
+352 451 454 920
tflamand@deloitte.lu



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



Michael JJ Martin
Partner - Forensic, AML & Restructuring
+352 451 452 449
michamartin@deloitte.lu



Jean-Philippe Peters
Partner - Business Risk/Risk & Capital Management
+352 451 452 276
jppeters@deloitte.lu



Xavier Zaegel
Partner - Capital Markets & Financial Risk
+352 451 452 748
xzaegel@deloitte.lu



Stéphane Hurtaud
Partner - Governance, Risk & Compliance
shurtaud@deloitte.lu
+352 451 454 434

Editorial committee



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



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

Deloitte is a multidisciplinary service organisation which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

Due to the constant changes and amendments to Luxembourg legislation, Deloitte cannot assume any liability for the content of this leaflet. It shall only serve as general information and shall not replace the need to consult your Deloitte adviser.

About Deloitte Touche Tohmatsu Limited:

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/lu/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 210,000 professionals are committed to becoming the standard of excellence.

