

Inside

CCO
CISO
CRO
CIA
BOD

EDITION
2 0 1 6



Top 10 for 2016
—Our outlook for financial
markets regulation

Bank board risk governance
—Driving performance through
enhanced risk oversight

Global risk management survey,
ninth edition—Operating in the
new normal: increased regulation
and heightened expectations

What are they saying?—New ways
to detect emerging reputation
(and other strategic) risks

Risk sensing—A tool to address
reputation risks

21st century resilience—Getting
it and keeping it

Focus on—Building crisis-ready
boards

Focus on—The board's-eye view
of cyber crisis management

The benefits and limits of cyber
value-at-risk

A holistic approach to regulatory
watch

Exponential Change
—Hot topics for internal audit
in financial services for 2016

Clarity, transparency and
comparability—The colors
of the PRIIPs Regulation

PSD2 opens the door to new
market entrants—Agility will be key
to keeping market position

Solvency II and Key Considerations
for Asset Managers

Transactions and Trade Regulatory
Reporting—A changing landscape

In this issue

6



22



36



46



56



60



4 Editorial

6 **Top 10 for 2016**
Our outlook for financial markets regulation

22 **Bank board risk governance**
Driving performance through enhanced risk oversight

36 **Global risk management survey, ninth edition**
Operating in the new normal: increased regulation and heightened expectations

46 **What are they saying?**
New ways to detect emerging reputation
(and other strategic) risks

56 **Risk sensing**
A tool to address reputation risks

60 **21st century resilience**
Getting it and keeping it

68 **Focus on**
Building crisis-ready boards

68

72

76

82

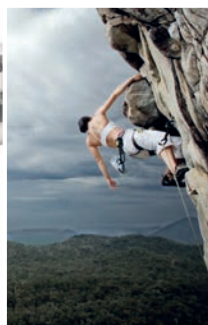
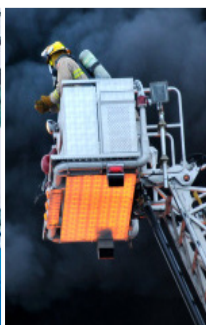
90

102

110

120

130



- 72 **Focus on**
The board's-eye view of cyber crisis management
- 76 **The benefits and limits of cyber value-at-risk**
- 82 **A holistic approach to regulatory watch**
- 90 **Exponential Change**
Hot topics for internal audit in financial services
for 2016
- 102 **Clarity, transparency and comparability**
The colors of the PRIIPs Regulation
- 110 **PSD2 opens the door to new market entrants**
Agility will be key to keeping market position
- 120 **Solvency II and Key Considerations for Asset Managers**
- 130 **Transactions and Trade Regulatory Reporting**
A changing landscape
- 134 **Contacts**



Dear readers,

Welcome to the second international edition of *Inside*, a publication dedicated to governing bodies and internal control functions. Our objective is to provide professionals involved in governance, risk, compliance, and internal audit with thoughtful insights into critical topics that may impact their organization.

Just like 2015, the year 2016 will see exponential change—organizations will need to keep abreast of technology developments, adjust to new regulatory requirements while meeting ever heightening stakeholder expectations, and managing emerging risks. Effective risk-sensing programs should be the cornerstone of companies that aspire to successfully manage strategic risks in the current environment, and internal control functions will need to adjust and adapt to the regulatory requirements, emerging risks, and competition within each industry. Threats like cyber risk are being exploited with greater frequency and to greater effect while customers expect greater digital capabilities. This change presents a unique opportunity for internal control functions to become a catalyst for change in their organization for the longer term.

Across the financial services industry, regulatory requirements are becoming broader in scope and more stringent. This year, the industry will continue to operate in a challenging environment due to continued advances in technology, adoption of new regulations, as well as competition from new entrants to the sector. The newly agreed upon Payment Services Directive 2, the entry into force of the Packaged Retail and Insurance-based Investment Products (PRIIPs), the data and regulatory reporting challenge (EMIR, MiFIR), and the go-live date for Solvency II, will create opportunities for companies that manage to turn compliance with new regulatory requirements into competitive advantage. Deloitte UK's 2016 regulatory outlook sheds further light on these topics and many others. In this edition, we have also gathered the results of Deloitte Touche Tohmatsu Limited (DTTL)'s Global risk management survey (ninth edition) and DTTL/Forbes Insights Risk Sensing survey that will provide you with information and key findings to help enhance your overall risk strategy and the related impact.

The main challenge for the financial services industry will be to find the right mix between compliance, risk management, and financial performance. 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 the right governance cultures. Driving performance through enhanced risk oversight and risk culture is a key element of each organization's success with the ultimate goal of creating shareholder value.

In an environment of continuing uncertainty and an elevated degree of regulatory risk, risk governance will continue to be a key driver in the development of your business strategies and models.

We hope you will find this publication insightful.

Sincerely,



Rick Porter
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



Top 10 for 2016

Our outlook for financial markets regulation

David Strachan
Partner
Co-Head EMEA Centre
for Regulatory Strategy
Deloitte UK

Clifford Smout
Partner
Co-Head EMEA Centre
for Regulatory Strategy
Deloitte UK

Julian Leake
Partner
Risk Advisory
Deloitte UK



Last year we¹ asked if in 2015 financial services firms would see the authorities shift toward promoting growth and implementing already agreed rules, and away from proposing new ones. As 2015 draws to a close, there is evidence of such a shift, especially within the European Union (EU). However, more generally, it has been post-crisis “business as usual”: daunting implementation challenges in respect of multiple regulations that affect financial services firms’ (particularly banks’) business models and strategies, significant unfinished business, especially in relation to bank capital, and an intensive supervisory and enforcement agenda.

Looking back

In 2015 three broad themes stood out. First, the political mood changed. The emphasis in the EU is now on the jobs and growth agenda; the flagship Capital Markets Union (CMU) initiative is more about deregulation than re-regulation. The shift in sentiment is even clearer in the UK, where the “tone from the top” from HM Treasury (HMT), the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) has changed significantly.

Moreover, even if the high level messages in the EU and the UK did change, on the ground the scale, scope and pace of regulatory, supervisory and, in some cases, enforcement activity were undiminished. In the meantime, firms have had to make progress with complex and inter-linked regulatory implementation projects which affect almost every aspect of their organization.

Second, progress in completing the extensive set of post-crisis regulatory reforms was slow. In the EU, legislation to deal with bank structural reform and money market funds stalled, while the timetable for some implementing measures of the Directive on Markets in Financial Instruments (MiFID II)² and benchmark reform slipped. The much-heralded end to the Basel policymaking agenda remained elusive.

It remains to be seen if this is a pause, reflecting the challenging nature of the open issues, or a more deep-seated impasse.

Third, there has been more emphasis on taking the system-wide perspective and asking questions about the cumulative impact of regulation. In this context, there are major unanswered questions about the consequences (intended and unintended) for market liquidity of a range of regulatory measures.

Looking forward

These themes will continue into 2016 and provide the backdrop for our predictions for the coming year.

We expect to see the trend of fewer brand new regulatory initiatives in the UK and elsewhere in the EU continue into 2016. Progress in completing “unfinished business” in the EU will be stately, leaving policymakers with a choice between delayed, or rushed, implementation.

There is also a question over the many open items on the agenda of the Basel Committee on Banking Supervision (BCBS). Much of the talk around this relates to comparability and consistency; certainly we do not anticipate much support for measures that raise capital requirements in ways that are viewed as undermining the EU’s jobs and growth mandate. Moreover, some senior policymakers have indicated that there should not be a major ratcheting up of capital for banks as a whole from the next set of changes. Until these residual (and significant) uncertainties are resolved, banks will be unable to take final decisions on their post-crisis business models and strategies.

We expect the authorities to continue to press for greater competition in financial services for the benefit of end users.

In the EU we expect the Commission’s plans for retail financial services to be heavily influenced by competition considerations. Moreover, the pace of technological development and innovation in financial services (“FinTech”) will continue to keep incumbents on their toes, as will challenger banks seeking to improve scale and operational leverage.

² At the time of finalisation of this document (2 December 2015) it looked as if there would be a delay in the “go live” date for MiFID II. At present there is no clarity as to the scope or extent of any delay. While we have prepared the document on the basis of a January 2017 “go live”, even if this date is pushed back, our view is that firms should, given the complexity of their implementation projects, press ahead where they are able to do so



That said, we expect further consolidation in banking markets, especially in continental Europe, driven both by overcapacity and vulnerabilities in banks' business models exposed by the low interest rate environment. In this context, for banks new guidelines on the Supervisory Review and Evaluation Process (SREP) in the EU come into force from 2016. Business models and business strategy – in terms of viability and sustainability – are core to the new paradigm of forward-looking supervision.

By now, over eight years after the onset of the financial crisis, we would have expected the policy making agenda to be largely complete. This is far from being the case: despite the enormous progress that regulators have already made, many loose ends remain. Moreover, there are reviews underway, especially in the EU, of aspects of the post crisis regulatory framework before the ink is barely dry.

This residual uncertainty has at least two consequences. First, it complicates and postpones some aspects of critical decisions that need to be made about strategy, business models and legal entity structure, especially by banks. Second, it pushes out the point at which financial services firms are able to focus more on how to extract business benefits from the significant investments they have made, often in haste, to comply with the plethora of regulatory requirements. However, as soon as the dust begins to settle, those firms which are best able to translate regulatory spend into either competitive advantage or lower cost structures will prosper. Last, but by no means least, we expect resilience – the ability of firms to prepare for, withstand and, if need be, recover from shocks – to be high among supervisory priorities in 2016.

The list of such possible event risks is long – cyberattack, geo-political instability, rising interest rates, the UK's referendum on EU membership ("Brexit"), the bond market's ability to absorb sustained selling – and growing. This will in turn put the spotlight on IT infrastructure, contingency planning, stress testing and on market-wide exercises to assess the resilience of individual firms and the system as a whole. "Be prepared."

So much for background. The top ten regulatory issues which we predict for 2016 are set out on the following pages, together with our views on how each will affect the retail banking, capital markets, insurance and investment management sectors. We have also suggested song titles that, for us, capture the spirit of the issue.

Some senior policymakers have indicated that there should not be a major ratcheting up of capital for banks as a whole from the next set of changes

1 Culture Respect

Larger firms will continue to grapple with defining and embedding a common culture, specifically one that resonates from the board and the top of the firm across all business areas and jurisdictions. Two key challenges will be to determine the levers that will encourage the right behaviors and to measure their effectiveness in facilitating cultural change.

Following the financial crisis, regulators have unleashed a number of initiatives to improve standards of conduct across the financial services industry. Changing culture is seen as key to this. We predicted last year that firms would struggle with the “how” of implementing culture – this looks set to continue well into 2016.

In the meantime, supervisors will continue to search for indicators of “good” culture – in particular the role of boards will be scrutinized, including their decision-making process, their focus on customer outcomes and managing conflicts of interest and the quality of Management Information (MI).

Remuneration will continue to be a key component to drive cultural and behavioral change as regulators continue their efforts to better align reward with risk and conduct.

De Nederlandsche Bank (DNB) currently leads the way in assessing culture through a three-tiered framework of behaviors (leadership, decision-making and communication), group dynamics (cohesion and interaction between individuals) and mindsets (values, convictions and attitudes that are regarded as important either individually or collectively). Other supervisors might well follow their lead.

The European Central Bank (ECB) is likely to push for more regulation to help drive harmonization in areas such as fit and proper assessments of board members where diverse national transpositions of the amended Capital Requirements Directive IV (CRD IV) make it impossible to achieve consistency across the Single Supervisory Mechanism (SSM).

2 Conduct risk Ain't misbehavin'

Firms will increase investment in resources and IT infrastructure to improve conduct risk surveillance and MI, to meet supervisory expectations and to avoid further problems, and the accompanying fines and reputational damage.

Conduct regulation will remain high on regulatory and supervisory agendas in 2016. In the UK, work will continue on flagship initiatives: implementing the results of the Fair and Effective Markets Review (FEMR), the SMR and SIMR, and the Financial Advice Market Review (FAMR). In terms of EU initiatives, all hands will be on deck to implement MiFID II, the Market Abuse Regulation (MAR) and the Regulation on Packaged Retail and Insurance-Based Investment Products (PRIIPs), at both regulators and firms. Conduct risk will be taken up by the global institutions to an extent not previously seen, with increased focus on integrating conduct risk into prudential frameworks and work by the International Organization of Securities Commissions (IOSCO), the Bank for International Settlements (BIS), and the Financial Stability Board (FSB) on benchmarks, an FX code, and the alignment of remuneration and conduct risk respectively.

Firms will seek to improve surveillance and MI to better manage conduct risk. They will try to be more forward-looking and outcomes-focused in their management of conduct risk, and will start looking for support in this from data analytics. Most firms will move toward embedding conduct risk in their risk management frameworks, although articulating conduct risk appetite will remain challenging. Across all sectors, product governance obligations will lead firms to seek increased information about each stage in the product lifecycle and to understand whether products are distributed to the target market for which they were designed.



Competition

Harder, Better, Faster, Stronger

While regulatory initiatives focused on competition will not lead to forced structural change or price regulation, regulators will continue to implement changes to improve competition. Consideration of competition issues will permeate and influence policy and supervisory decisions. 2016 will be the year when firms need to review and understand the costs for each product and how these costs are disclosed to the customer, leading to increased transparency, reduced product bundling, and cross-subsidisation. MiFID II, IDD, and FCA market studies into investment banking and asset management are the main drivers for this change. And the FCA is also concerned about the value for money that consumers derive from financial services. As a consequence, firms will need to evaluate their product and service offerings.

The regulators are looking to improve competition in financial services through encouraging and facilitating innovation. Regulatory actions to promote competition will extend beyond financial services firms and to the institutions and infrastructure that support them. Crowd funding, peer-to-peer lending and foreign exchange transfers appear to be the biggest disrupters within FinTech.

However, regulators, in the EU and the UK will exert most of their effort on payments systems in 2016. The revised Payment Services Directive, expected to come into force in 2017, will open the payments market to competition from non-bank players and will force banks to make clear decisions about their strategic response.

The European Commission's Green Paper on retail financial services and insurance, expected to be published in December 2015, is seeking to build a genuine Single Market by increasing competition and improving consumer choice in all sectors. The review will also look at the impact of digitalization in the market and how new distribution channels can improve competition. We will need to wait and see how the European Commission will move forward with this project, but it is clear that improving competition is a priority at both the EU and UK level.

2016 will be the year when firms need to review and understand the costs for each product and how these costs are disclosed to the customer, leading to increased transparency, reduced product bundling, and cross-subsidisation





Structural reform

Breaking up is hard to do

Delivering structural reform in financial services has proceeded in fits and starts. In 2016, resolvability will increasingly drive regulatory interventions as authorities focus on the practicalities of resolution planning. For banks in particular, there will be increased focus on what is being done to ensure operational continuity.

Global systemically important banks (G-SIBs) are at the top of the action list. Work has progressed in Crisis Management Groups, but the FSB recently said that “significant work remains” in order to make resolution plans operational. Within the EU the UK authorities will continue to lead the way.

The focus will be on operating models, and “operational continuity” will be a motivating factor for a range of initiatives. Within the Banking Union, the new Single Resolution Board (SRB) will have to come to grips with the roughly 150 banking groups within its remit. In 2016 the SRB is more likely to be gathering information than requiring banks to restructure.

The globally agreed standard for Total Loss-Absorbing Capacity (TLAC) was “finalized” in November 2015, but left many questions to be answered on a bank-by-bank basis. Investors will want to understand their position in the creditor hierarchy, forcing banks to be more transparent, with possible consequences for their funding costs.

The work on TLAC – implemented as the Minimum Requirements for Own Funds and Eligible Liabilities (MREL) in the EU – may act as a link between resolution issues and those relating to prudential requirements more generally.

The EU’s attempts to implement its own framework for bank structural reform will progress slowly as EU Member States continue to disagree about the proposed Regulation. If the Regulation is agreed upon in 2016, we would expect a framework which closely ties resolvability to the separation of trading from retail deposit-taking.



Measuring risk exposures

Let’s twist again

New proposals being developed for the measurement of risk exposures will have a widespread impact and place significant new demands on firms, both in terms of the capital required to be held and the systems and processes needed to calculate the requirements.

Even as the overall shape of the new regulatory regime settles down, policymakers are developing a broad range of proposals that set in their crosshairs the consistency, comparability and transparency of risk weights across different types of risk and between institutions. The effect on firms will vary by business model, and according to their current approach to regulatory capital modelling.

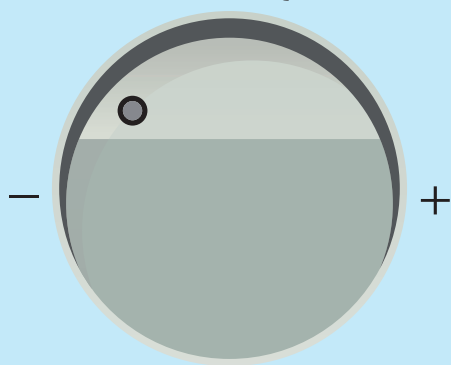
Changes to date to prudential capital requirements have focused on the absolute level of capital held. The interest in how much capital is held against different risk exposures will have implications for the overall requirement, but is primarily concerned with ensuring that regulatory incentives to take one risk over another are not skewed, for example by a particular modelling approach.

In some cases, there is also concern from regulators and legislators about the potential for misalignment between the regulatory capital agenda and the broader political interest, particularly in the EU, in promoting financing for businesses to accelerate economic recovery. The outcome of the European Commission’s consultation on the possible impact on bank financing of the economy, and its call for evidence on the EU regulatory framework for financial services more broadly, will be instrumental in setting the policy direction for future capital requirements in the EU.

A related concern that more complex requirements will raise barriers to new entrants and/or stifle competition from existing challenger banks is exercising policymakers, including the PRA in the UK, and will weigh on the form of the final solution.



Volume



Pitch adj.



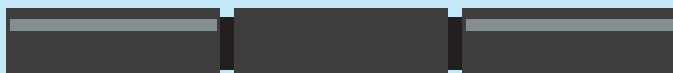
Power



45

33

78



Market participants adjusting to a new order

The times they are a changin'

Uncertainty over future market structure and dynamics will persist as prudential and collateral rules bite deep and transaction costs for trading activities continue to increase. The seeds of significant change will be sown in 2016 for trading across all instrument classes, affecting both pre- and post-trading structures.

Operational resilience

Livin' on a prayer

Supervisors will pay increasing attention to operational resilience.

The spotlight will be on risk identification and mitigation, contingency planning, stress testing and on market-wide exercises (such as the recent UK-US joint cyber-incident exercise with major financial institutions) to assess the resilience of individual firms and the system as a whole.

Technology and innovation

Under pressure

Technology must remain close to the top of firms' agendas in 2016. Established players will need to invest in technology, not only to satisfy the demands of their supervisors, but also to compete. If they don't, they will see their business shrink. Innovators will increasingly have the ear of politicians and supervisors.

Data and regulatory reporting

I still haven't found what I'm looking for

Firms can deal with data by investing heavily now to realise the long-term benefits, or by using ever-bigger "sticking plasters".

The ultimate winners will be firms that bite this bullet soon. In 2016 this will become much more apparent as the number and overall complexity of demands on firms increase further, and supervisors spend more time assessing firms' capabilities.

Capital calibration

Get the balance right!

After several years of changes to the make-up of the regulatory capital regime, in 2016 the focus will be on the calibration of the overall framework, and the distribution of capital between firms. That said, there remains significant uncertainty about just how many elements of the debate will be finalised in the coming year.

Top 10 f
Our outl
financial market

Culture

Respect

Larger firms will continue to grapple with defining and embedding a common culture, specifically one that resonates from the board and the top of the firm across all business areas and jurisdictions. Two key challenges will be to determine the levers that will encourage the right behaviours and to measure their effectiveness in facilitating cultural change.

Conduct risk

Ain't misbehavin'

Firms will increase investment in resources and IT infrastructure to improve conduct risk surveillance and MI, to meet supervisory expectations and to avoid further problems, and the accompanying fines and reputational damage.

Competition

Harder, Better, Faster, Stronger

While regulatory initiatives focused on competition will not lead to forced structural change or price regulation, regulators will continue to implement changes to improve competition. Consideration of competition issues will permeate and influence policy and supervisory decisions.

Structural reform

Breaking up is hard to do

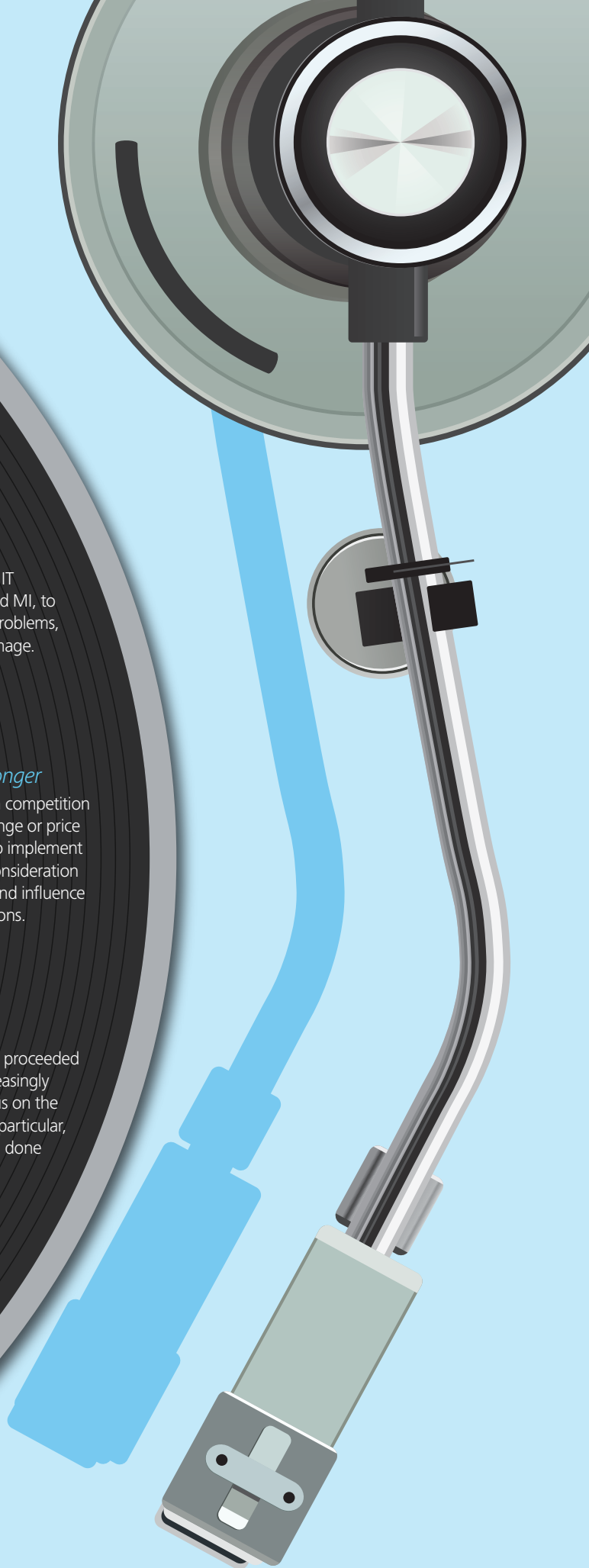
Delivering structural reform in financial services has proceeded in fits and starts. In 2016, resolvability will increasingly drive regulatory interventions as authorities focus on the practicalities of resolution planning. For banks in particular, there will be increased focus on what is being done to ensure operational continuity.

Measuring risk exposures

Let's twist again

New proposals being developed for the measurement of risk exposures will have a widespread impact and place significant new demands on firms, both in terms of the capital required to be held and the systems and processes needed to calculate the requirements.

ook for 2016
ook for
ets regulation





Capital calibration

Get the balance right!

After several years of changes to the make-up of the regulatory capital regime, in 2016 the focus will be on the calibration of the overall framework, and the distribution of capital between firms. That said, there remains significant uncertainty about just how many elements of the debate will be finalised in the coming year.

The calls for more and better quality capital were easy to make in 2008 as the financial crisis unfolded and undercapitalization was seen as a root cause of the failure of individual firms, and of the systemic contagion that unfolded. Roll the clock forward to now and the considerations are more complex. There is a growing constituency for reviewing whether new requirements have “overshot.” Initiatives such as the Bank of England (BoE)’s Open Forum (and the follow-up it will catalyse), the EU’s CMU, and the European Commission’s consultation on the impact of capital requirements on the economy, tackle inter alia concerns – which to some policymakers are misplaced – that regulation is constraining economic growth.

There are related questions about how different but connected changes to the regulatory framework interact, the possibility of double-counting of risks, and whether there have been any unintended consequences.

Mark Carney, Governor of the BoE and Chair of the FSB, has noted that “given the complexity and scale of financial reform, it would be remarkable if every measure were perfectly constructed. Or if they all fit[ted] seamlessly into a totally coherent, self-reinforcing whole.”

In the UK, the Financial Policy Committee (FPC)’s paper in December 2015 on the framework of capital requirements for UK banks tackled some of these themes.

In this respect, the growing importance of stress testing as a lever for supervisory risk assessment is an important consideration. More broadly, changes to accounting standards, changing practices around risk modeling and efforts to improve the resolvability of financial institutions, amongst others, need to be weighed against judgments on the right level of regulatory capital buffers in order to understand aggregate capital requirements.



Data and regulatory reporting

I still haven’t found what I’m looking for

Firms can deal with data by investing heavily now to realize the long-term benefits, or by using ever-bigger “sticking plasters”. The ultimate winners will be firms that bite this bullet soon. In 2016 this will become much more apparent as the number and overall complexity of demands on firms increase further, and supervisors spend more time assessing firms’ capabilities.

Regulators and supervisors want financial services firms to provide them and the firms’ clients and customers with better quality data, more quickly and in a format that is more easily interrogated.

They are also setting new expectations for how firms manage data for their own purposes. Supervisors need the information to assess risks and to police compliance with an ever-more-complex regulatory framework. Greater transparency for the public is considered key to enabling real choice and ensuring fair treatment.

This trend has been clear for several years, but relatively limited progress has been made towards meeting expectations. In part that is because the end state is still evolving, as new requirements are introduced. It is also because of the complexity and cost of the remediation work required to firms’ systems and operations; and the cost of fulfilling requirements (including, sometimes, reporting to different bodies for the same topic but using different templates).

From an implementation perspective, major challenges arise from the definition of a firm-wide data policy and data dictionary, and from the need to integrate risk and finance data. Any solution will require looking for innovative ways through the challenges. Firms should also consider how investment to meet regulatory requirements can be leveraged to tackle the need to deal with the ever-increasing quantity of data being generated and the expectations of clients and customers to deliver a personalized digital experience. That said, firms will need to grapple with the implications of the EU General Data Protection Regulation and 'Safe Harbour 2.0' in 2016, which may be a counterweight to a desire to integrate and consolidate data sources.



Technology and innovation Under pressure

Technology must remain close to the top of firms' agendas in 2016. Established players will need to invest in technology, not only to satisfy the demands of their supervisors, but also to compete. If they do not, they will see their business shrink. Innovators will increasingly have the ear of politicians and supervisors.

Lack of investment in the past decades has left many financial institutions with the legacy of "unfit for purpose" IT systems, as discussed in the "Data and regulatory reporting" section. Not only do these create exposure to costly IT "glitches", and cyber-attacks, but they also expose them to fierce competition from new FinTech startups. The good news is that through investment in technologies, incumbents can respond effectively to these challenges. Strategic partnerships with FinTech startups will also be part of the solution.

Technology, as well as being a challenge, also promises to help firms solve some of the issues they are facing. RegTech innovations marry technology and regulation and will help firms investing in them to manage their regulatory compliance responsibilities cost effectively by making it easier to identify risks and improve efficiency.

Regulators and supervisors want financial services firms to provide them and the firms' clients and customers with better quality data, more quickly and in a format that is more easily interrogated

But it is not only financial services firms which are being "disrupted". Technology is challenging the way regulators think and operate. In particular, whereas overall technology has improved access to financial services (especially in developing countries), there are important unanswered questions around the adequacy of consumer protection and profiling, as well as data privacy issues.

Regulators will need to develop the capabilities to understand, respond, and leverage new technological developments, e.g. Blockchain, and the risks they pose without stymieing innovation. The FCA is leading this effort through "Project Innovate" which is designed to support new and established businesses understand the regulatory framework and how it applies to new innovations.

More generally, we expect to see competition developing between countries as the authorities seek to make their financial centres and regulatory frameworks "FinTech friendly" to attract new business.



Operational resilience

Livin' on a prayer

Supervisors will pay increasing attention to operational resilience. The spotlight will be on risk identification and mitigation, contingency planning, stress testing and on market-wide exercises (such as the recent UK-US joint cyber-incident exercise with major financial institutions) to assess the resilience of individual firms and the system as a whole.

Operational resilience is the ability of financial services firms and the financial system as a whole to withstand and, if need be, recover from crystallized event risk. Its focus is predominantly on the critical functions and services that firms provide, both in terms of the functioning of the financial system (including the “plumbing”, e.g. in relation to payments and settlement systems) and ultimately to the real economy itself.

There are two broad reasons for this heightened supervisory interest. First, IT is playing an even greater role in the services that firms provide (e.g. through increasing automation of previously manual process and through digital service channels), thereby increasing dependencies on the resilience of IT infrastructure.

Second, the level of threat is increasing. The vulnerability of financial services firms to cyber-attack is gaining increasing public and political prominence. At the same time there is no shortage of other possible “event risks”, whether from the current, increasingly fragile, geo-political situation in some regions, possible market reaction to rising interest rates, “Brexit”, the bond market’s ability to absorb sustained selling and so on.



The vulnerability of financial services firms to cyber-attack is gaining increasing public and political prominence



Market participants adjusting to a new order

The times they are a changin'

Uncertainty over future market structure and dynamics will persist as prudential and collateral rules bite deep and transaction costs for trading activities continue to increase. The seeds of significant change will be sown in 2016 for trading across all instrument classes, affecting both pre- and post-trading structures.

Uncertainty will reign, both in understanding how to implement the plethora of new regulatory requirements introduced following the financial crisis but also in understanding the cumulative effect on market dynamics. While the consequences of the individual regulatory changes were clearly intended and thought through, some of the others, particularly those consequences arising from their cumulative effect, may well be unintended. This uncertainty is clearly vexing policymakers, with the FSB, European Commission, ECB and BoE all advocating further work to understand the complex factors at work.





Concerns around fragile market liquidity will be compounded by additional regulatory pressures, such

as the penalties introduced by the Central Securities Depositories Regulation (CSDR) for settlement failure, which could serve to further disincentivize market makers in addition to existing prudential restrictions. All market participants will face increased pressure to consider how they will manage sudden shifts in liquidity.

Firms will be gearing up for the "go live" date of MiFID II, and implementation programs will need to tackle known challenges such as how to meet best execution requirements in over-the-counter markets. Expect to see the start of a proliferation of new trading venues over the next year or so. At least in the near-term, reduced liquidity in fixed income markets, in some part caused by capital and liquidity requirements on the sell side, are likely to result in reduced trading.

The European Market Infrastructure Regulation (EMIR) will be a significant cost as the final and most onerous provisions come into effect. The introduction of the clearing obligation will lead to significant variation in pricing, and the margining requirements will only add to the existing regulatory pressures for eligible collateral and will compound the demand for high quality liquid assets. Sourcing collateral is likely to be more difficult than ever before.

Top 10 for 2015 - *How did our predictions fare?*

 Topic	 What we said	 What happened	 Score out of 10
Structural reform and resolution in the financial sector	<ul style="list-style-type: none"> The resolvability agenda should be watched closely It will be an intense year for UK ring-fencing Uncertainty hangs over the EU Bank Structural Reform (BSR) 	<ul style="list-style-type: none"> In the UK a number of crucial PRA secondary standards were issued Submission of RRP (UK). The development of loss absorbency rules (EU/FSB) has continued EU Member States have struggled to address the issue of subordination of bail-inable liabilities in MREL and TLAC The Council of the EU has agreed its position on BSR, but ECON divisions delayed progress on the file 	9
New institutions in action	<ul style="list-style-type: none"> The SSM will be a sharp learning curve for eurozone banks The Single Resolution Mechanism (SRM) will get up and running The new European Commission will step up its focus on economic growth 	<ul style="list-style-type: none"> As the SSM gathers speed, banks face multiple layers of supervision Uncertainties around how the SRM will work, in part due to delays in the BRRD The European Commission has indeed shifted its focus toward growth 	8.5
Data and regulatory reporting	<ul style="list-style-type: none"> Supervisors' appetite for data shows no sign of abating Banks should look beyond the follow-up to asset quality review (AQR) to RRP and data aggregation There is increasing emphasis by supervisors on process as well as outcome 	<ul style="list-style-type: none"> All the initiatives identified at the start of the year came to pass, and more. Supervisors' expectations on data continued to expand, and the focus on method as well as outcome was there Despite those developments, there is no impression of a big turning point in the approach banks are taking, nor of supervisors pushing banks to develop strategic solutions – yet 	8
Culture and treatment of customers	<ul style="list-style-type: none"> Firms must “do” culture, not just talk about it Supervisors will expect to see evidence of progress SMR will focus individuals' attention It is increasingly important for firms to produce reliable conduct risk “data” 	<ul style="list-style-type: none"> “Doing” culture has been a focus of SMR and new PRA governance rules, and will be the subject of an FCA thematic review The FEMR delivered 21 wide-ranging recommendations for FICC markets, with focus on individual and collective accountability and firms identifying and managing their conduct risk 	9.5
Competition and innovation	<ul style="list-style-type: none"> 2015 will bring clarity on the FCA and CMA's concurrent competition powers Competition will be prominent at the EU level Regulators' competition-related work will likely have implications for strategy and business models 	<ul style="list-style-type: none"> As part of its new role, the FCA published the wholesale sector competition review The FEMR, Payment Systems Regulator (PSR) and the European Commission have all prioritized competition CMA published a provisional report on retail banking. It did not suggest any structural changes, and left some stakeholders unimpressed FCA interim findings of its credit card market study found competition worked well in most of the market. The remedies focussed on long-term debt and helping consumers find the best deal 	6.5



Topic



What we said



What happened



Score out of 10

Stress testing and risk management

- Stress testing will become an increasingly important supervisory tool
- Firms need to be thinking about a “one firm” approach
- Murmuring about cross-border coordination of stress testing will get louder

- 2015 exercises in the UK and US pushed banks to higher standards as expected, and the trend is set to continue
- EBA’s SREP guidelines, now being implemented, codify the importance of stress testing as a core component of supervisory analysis.
- International alignment still mentioned, but no concrete steps forward, and the prospects do not look favorable

8.5**Capital markets union**

- CMU is a flagship new agenda for the Commission.
- Questions remain, including how it will interact with existing initiatives.
- CMU will be well debated as stakeholders vie to influence the agenda.

- Following an avalanche of responses to the Green Paper and vocal debate, the CMU action plan was delivered with 33 initiatives.
- There is consultation on the first wave of initiatives
- The CMU is set to be rolled out over the next four years

10**Business model mix**

- Managing the implications of ongoing changes to the Basel framework is a strategic challenge
- Devising a business model that leverages spend on regulatory change is key

- Many banks continue to re-evaluate their mix of activities/business lines in which they operate
- The primary driver is often given as cost, however reducing capital requirements is frequently a major target
- Supervisors’ awareness of the aggregate implications of regulatory requirements is increasing, as evidenced by the publication in 2015 of the EBA’s “Overview of the potential implications of regulatory measures for banks’ business models”

7**Solvency II and insurance capital**

- Implementation of Solvency II (SII) will enter its final year
- Solvency II will raise questions on insurers’ business model mix
- Work on a global ICS is gaining steam

- Work on the ICS is delayed by a year and due to be completed in Q4 2019
- Development of HLA was endorsed by G20
- PRA is expected to communicate the results of the internal model approvals in early December 2015 ahead of the “go live” date

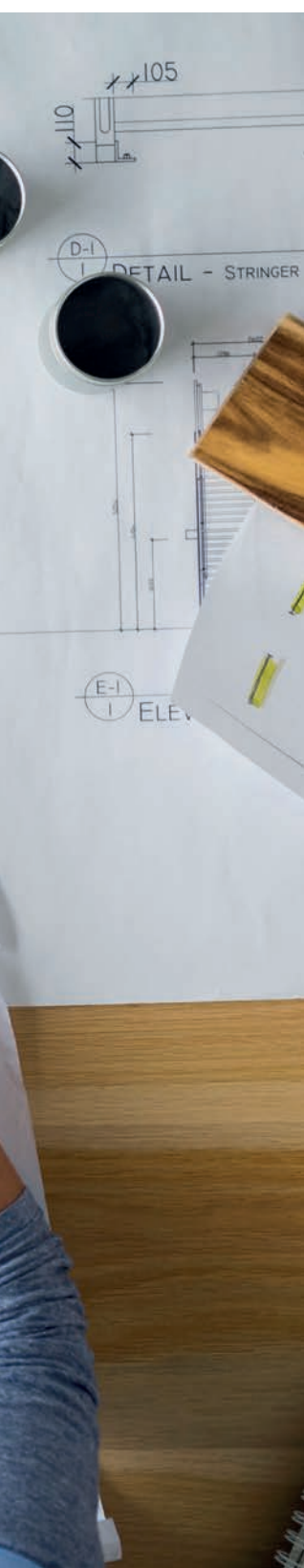
7**The interaction of market structures**

- Financial market structures will be radically altered by regulatory requirements
- Issues on extraterritoriality will not go away
- Transatlantic Trade Investment Partnership (TTIP) will be one to watch
- Debate will continue on the technical details of MiFID II

- There have been further delays to the US equivalence decision although significant progress has been made on equivalence for other jurisdictions leading to the recognition of the first third country CCPs
- There are clear indications of fragmentation in derivatives markets
- The MiFID II RTS have been delayed in the form of Delegated Acts, leaving the market without clarity on key details
- In the TTIP negotiations, no concrete solutions have been found with respect to the framework for regulatory cooperation on financial services

7





Bank board risk governance

Driving performance through enhanced risk oversight

Scott Baret
Partner
Banking & Securities Leader
Deloitte US

Val Srinivas
Senior Manager
Research Leader
Banking & Securities
Deloitte US

Lincy Therattil
Manager
Banking & Securities
Deloitte US

Urval Goradia
Senior Analyst
Banking & Securities
Deloitte US

During six consecutive quarters in 2013 and 2014, two groups of large US banks showed substantially different operating results. The average Return On Average Assets (ROAA) in one group was 57 percent higher. Otherwise—in terms of average total assets and other characteristics—the two groups were roughly similar.

A look at board risk committee charters of large banks

One key difference between the two groups was that the board risk committee charters of the higher-performing banks documented the need for a risk expert.¹

Of course, correlation does not mean causation, and because it is only in recent times that the more rigorous risk governance practices have been introduced, it will be a while before one can examine the long-term relationship between robust risk governance and financial performance. Requiring a risk expert on the board risk committee is just a strong sign of a bank's commitment to risk management and governance, which, in theory, can exert positive influence on performance.

Many banks seem to have taken this lesson to heart. Efforts to strengthen risk management and instill appropriate policies and a risk intelligent culture throughout the organization have become top priorities for many banks. Major failures in risk management and oversight, some carrying heavy costs, show the stakes are high. Board risk committees, as the highest level of risk oversight, and crucial promoters of the "tone at the top," are increasingly focused on this transformation.

Regulatory expectations in the area of risk management are only adding to the pressures flowing from other regulations. In particular, in the United States, the

Federal Reserve's Enhanced Prudential Standards (EPS) require bank holding companies to have additional risk governance standards in place as of January 1, 2015—a key driver of recent efforts. Internationally, the European Union's Capital Requirement Directive IV is likely having a similar impact on bank boards' risk governance practices.²

Another driver is the revised set of principles on bank corporate governance issued by the Basel Committee on Banking Supervision, which also encourage greater board-level risk oversight.³

In meeting these new standards, banks will need to show not only technical compliance with policy and process requirements, but also, increasingly, that their board risk committees are capable of presenting effective challenges to management decisions as part of their oversight duties. This is also stipulated by the Office of the Comptroller of the Currency's (OCC) Heightened Standards. In other words, these regulations have increased both director responsibility and potential liability.

Examining the board risk committee charters of bank holding companies enables us to make more informed evaluations of the current state of risk oversight, and provide some insight into the challenges banks face as they strive to comply with these new regulatory mandates.

An essential foundation of strong board-level oversight

We acknowledge that charters might not fully reflect all the actions, policies, and activities that board risk committees in these institutions actually follow. Likewise, there might be items in the charters that are not implemented in practice. As such, we suggest that our results be interpreted in that light. However, we believe that comprehensive, clear, and accurate risk committee charter documentation is an essential foundation of strong board-level oversight.

¹ This finding, drawn from analysis of our board risk committee charter research (see research methodology below) and SNL Financial's database, is limited to the set of banks studied during 2013-1H2014 period only. It is possible that there are other factors that contributed to the differences between the two groups of banks, but these were not readily apparent to us from the data. Read the paper on dupress.com for more detailed findings

² "Capital requirements regulation and directive – CRR/CRD IV," 11 November, 2014, http://ec.europa.eu/finance/bank/regcapital/legislation-in-force/index_en.htm

³ Basel Committee on Banking Supervision, "Corporate governance principles for banks - consultative document," October 2014

⁴ In this paper, the term "leading practice" refers to risk policies, procedures, controls and frameworks that are not yet widely adopted in the marketplace, and are indicative of a higher level of risk governance maturity

⁵ Federal Reserve, "Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations: Final Rule," 27 March, 2014

⁶ G-SIBs identified using the Financial Stability Board's November 2013 list



Board risk committee charter analysis

The Deloitte Center for Financial Services developed a list of 25 criteria applicable to board risk committee charters. These criteria are based on a wide range of regulatory requirements and leading practices⁴ identified by subject matter specialists, but, in particular, draw on the requirements of the Federal Reserve's "Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations."⁵

In conducting our research we obtained the following documents, where publicly available:

1. Board risk committee charters of US financial holding companies with assets greater than US\$50 billion as of 31 March, 2014, according to the Federal Financial Institutions Examination Council (FFIEC). Savings and loan holding companies were

omitted because they are not subject to the same regulatory risk management requirements as bank-affiliated financial holding companies

2. Risk and/or hybrid board risk committee charters, or similar documents, where available in English, of all non-US G-SIBs⁶
3. Board risk committee charters of US non-banks that have been designated systemically important financial institutions (SIFIs) by the Financial Stability Oversight Council

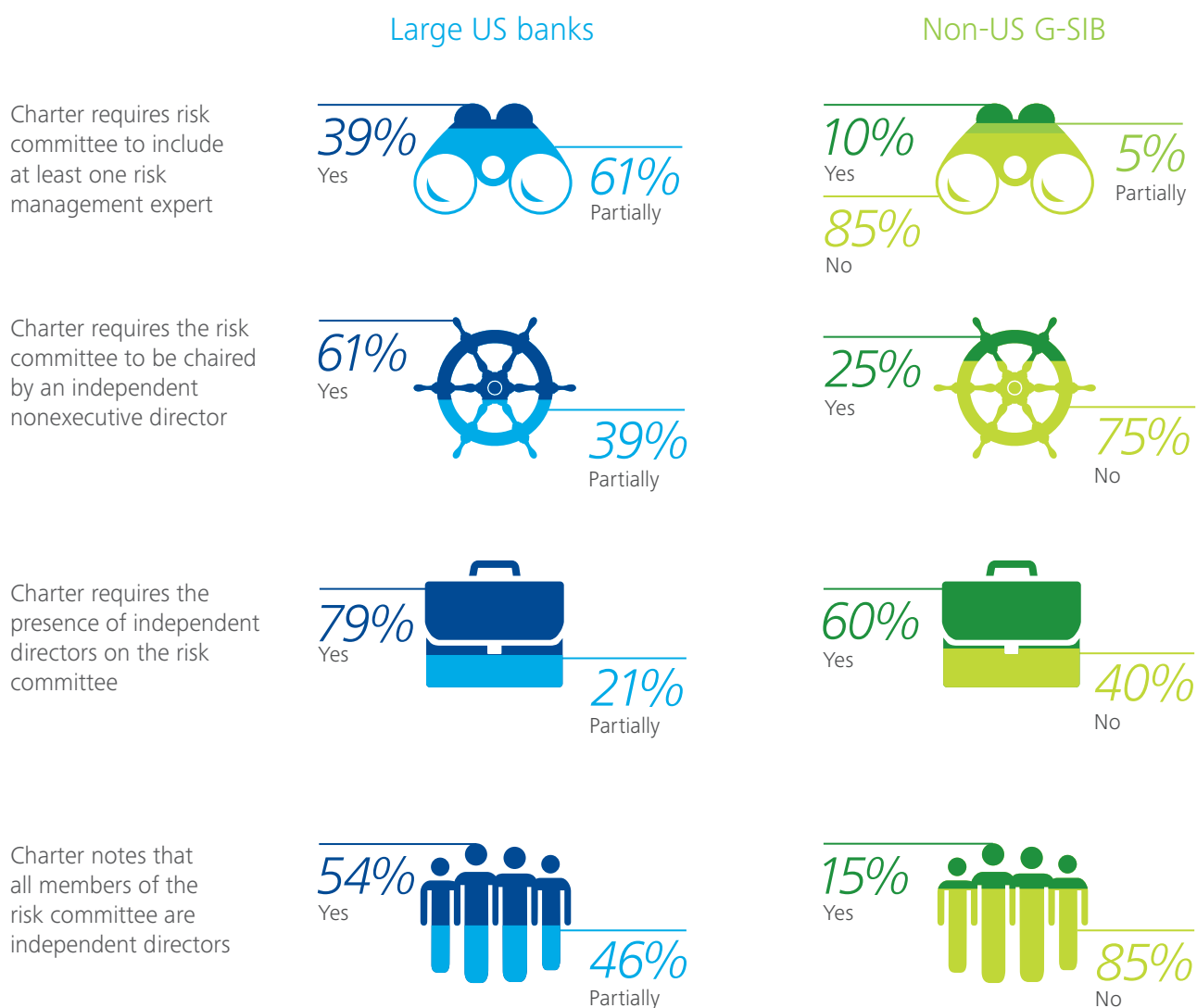
In total, 48 board risk committee charters were reviewed and assessed using the attributes listed in the paper to determine whether or not the charter met each criterion. The assessments were performed from August through September 2014 using the latest, publicly available documentation.

1. Evolving bank board risk committees: trends and findings

Continuing evidence of recent risk-management lapses have increased regulatory pressure. More stringent rules mandate new attention to structure, membership, reporting lines, and independence of bank boards and their risk committees.

Membership: room for improvement in expertise and independence requirements

Figure 1: Board risk committee membership



Source: Bank board risk committee charters and Deloitte Center for Financial Services analysis

As much as the scope of the committee matters, its composition may matter more. Committee members without the right mix of expertise and experience may be challenged by complex risk measures and regulatory issues.⁷ Board risk committees without sufficient numbers of independent members may run afoul of regulatory mandates. More importantly, these shortcomings might limit board risk committees' ability to offer the perspective needed to avoid potentially costly gaps in oversight.

Looking again to board risk charters for evidence, it appears many US banks have missed the opportunity to document the composition of their risk committees (Figure 1). Just 39 percent of board risk charters require a committee member to have the "experience in identifying, assessing, and managing risk exposures

of a large, complex financial firm," as required by the Federal Reserve's EPS. But there has been much improvement: in 2011, the last study we did of board risk committee charters, no banks had this requirement. A smaller percentage of non-US G-SIBs have specifically addressed this issue: only 15 percent of their charters mention risk expertise.

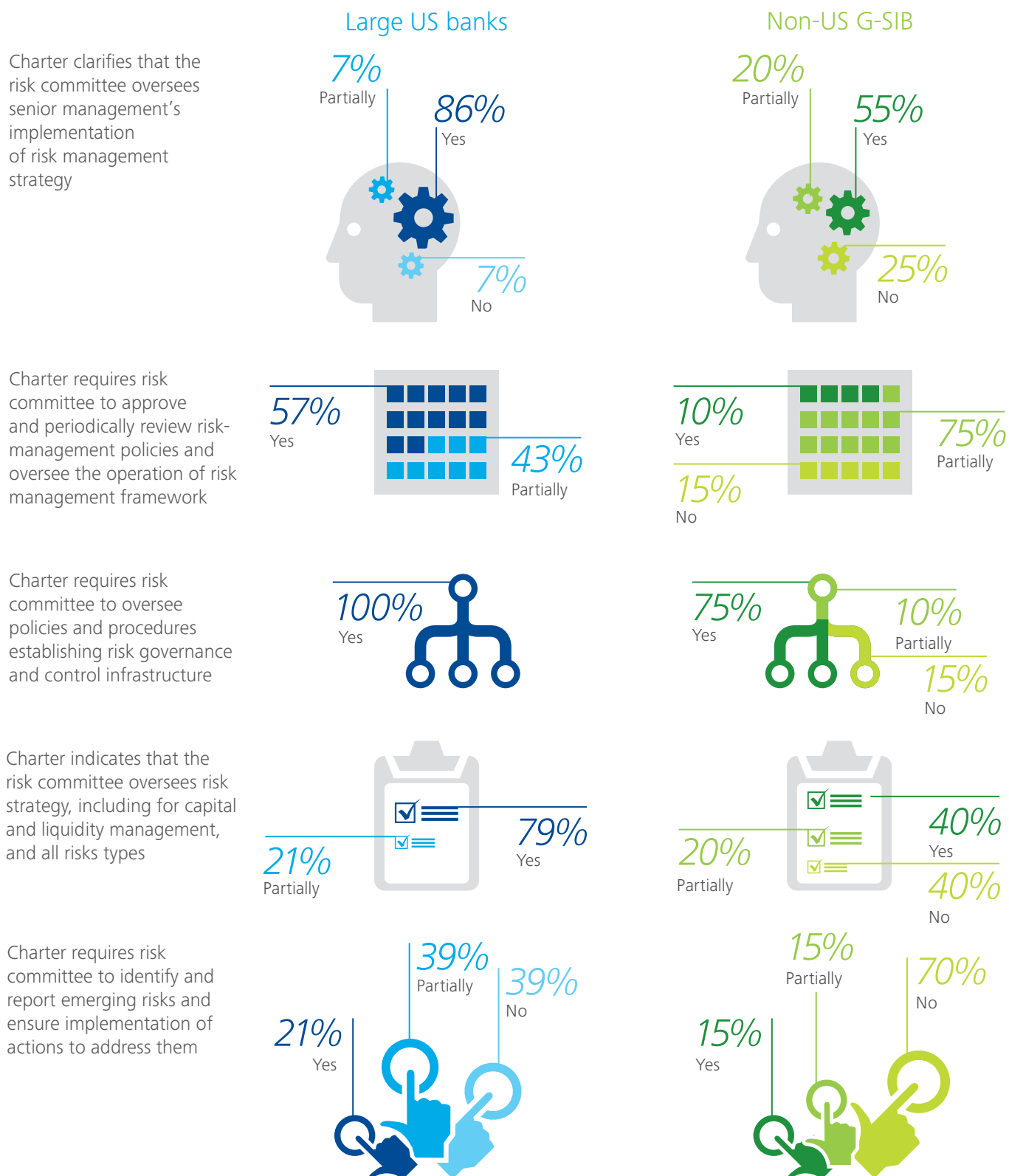
That said, both US banks and non-US G-SIBs appear to have taken steps to strengthen the independence of the committee. Nearly four in five US firms reviewed have documented a requirement for one or more independent directors on the risk committee, as do 60 percent of non-US G-SIBs. In our 2011 study, just 30 percent of US banks documented requiring an independent director.



⁷ For bank holding companies with assets greater than US\$50 billion, the Federal Reserve's Enhanced Prudential Standards define a risk management expert as someone with "experience in identifying, assessing, and managing risk exposures of large, complex financial firms."

Increased responsibilities and scope of oversight

Figure 2. Board risk committee responsibilities



Source: Bank board risk committee charters and Deloitte Center for Financial Services analysis

To respond to their expanded responsibilities, board risk committees have seen an increase in the depth and breadth of their oversight authority. The heft of new requirements and notable performance difficulties have drawn focus to this issue. This is particularly noted in banks' efforts to meet the "effective challenge" standard expected by US regulators. (In brief, the "effective challenge" standard requires risk management practices to be critically examined by oversight bodies with sufficient competence, power, and incentives to generate change.⁸)

The impact of increased expectations is gradually becoming visible in board risk charters (Figure 2). 100 percent of US banks' board risk committee charters and 75 percent of non-US G-SIBs' charters now require the board risk committee to oversee policies and procedures establishing risk-management governance and risk-control infrastructure (Figure 1).

This is also evident in the breadth of risks covered by the committee. Nearly 80 percent of US banks' board risk charters make committees responsible for oversight of exposure to a set of risk categories including not only credit risk, market risk, and operational risk, but also liquidity risk, reputational risk, and capital management.

However, only 57 percent of US banks' board risk charters place the responsibility to approve the firm's broad risk management policies with the board risk committee. This fact indicates that the board risk committees in nearly half the firms reviewed may be missing a key oversight mechanism. Still, US firms are significantly further ahead of their non-US counterparts in this respect: only 10 percent of non-US G-SIBs have such stated approval authority.

Nearly four in five US firms reviewed have documented a requirement for one or more independent directors on the risk committee, as do 60 percent of non-US G-SIBs

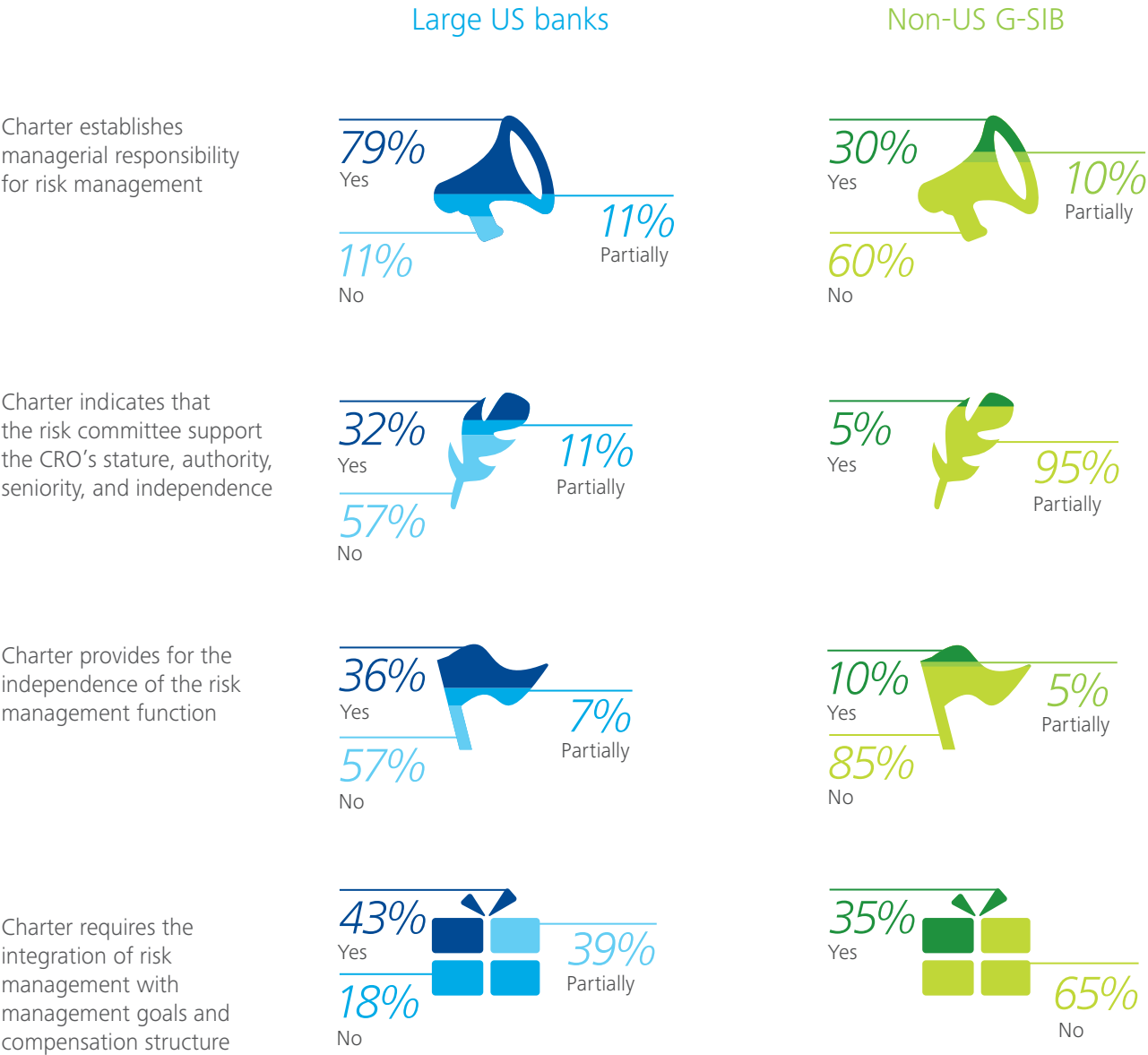
Risk oversight also seems to be rather reactive. Only one in five US bank risk committee charters (a) specify that alerts on emerging risks should be provided to the board risk committee and (b) authorize the committee's oversight of timely and effective remediation by management. Non-US G-SIBs show similarly muted resolution, with only 15 percent of their charters mentioning the communication of emerging risks and oversight of remediation. In other words, this is an area where there appears to be room for improvement.

This comprehensive oversight can give committee members greater understanding of the interplay of risks to which the firm is exposed, while giving them the focus needed to make sure they address emerging issues promptly.

8 "Supervisory Guidance on Model Risk Management," Federal Reserve and OCC, 4 April, 2011

Role in promoting independence of the risk management function

Figure 3. Board risk committee’s role in protecting independence of CRO and risk management function



Source: Bank board risk committee charters and Deloitte Center for Financial Services analysis

Board risk committee charters indicate that many institutions take this responsibility seriously, but our study finds that US banks may need to make progress before they can sufficiently satisfy regulatory expectations—or at least better document the steps they have already taken. Most board risk charters of domestic banks either directly or indirectly establish management’s responsibility for managing risk and the risk committee’s oversight of this responsibility (Figure 3). However, only just above a third explicitly highlight the committee’s role in requiring and fostering the independence of the risk management function.

Organizational reporting—both in terms of reporting lines and timing of formal reports—are a potential weak link in adequately supporting the risk management function. The board risk charter analysis indicates that establishing norms and safeguarding communication may be challenging banks. Only 36 percent of US firms’ board risk charters explicitly require the CRO to report on risk management to the committee on at least a quarterly basis. Similarly, just 36 percent of board risk charters state that the CRO reports directly to both the risk committee and the bank’s CEO. Both of these are governance expectations of the EPS.

Two other findings further identify places where banks can improve. First, only 32 percent of US banks’ board risk charters have language indicating that the board risk committee actively supports the role of CRO such that the CRO has the independence and authority to fulfill his or her responsibilities. For example, the charter may specify that the board risk committees may review the CRO’s hiring, compensation and incentive structure, and dismissal; may verify his or her freedom

of action; and may take similar steps. This is a modest improvement from the 15 percent recorded in 2011, but could be higher and better documented. Second, only 11 percent of US banks’ board risk committee charters document the ability of the CRO or other risk officers to communicate on an unscheduled basis with the committee. Progress in this area has also been modest for the global banks included in the study.

Role in driving risk awareness and culture

Setting the right tone at the top is critical for firms’ efforts to improve risk management. But the lack of board-level documentation supporting the alignment of risk with incentive structures shows a missed opportunity to reinforce this tone. Our board risk committee charter analysis suggests that only 43 percent of US banks have mandated integration of risk management concerns into compensation, a regulatory requirement and one that is essential to strengthening firm wide risk culture.

2. Overcoming challenges in board risk governance

Now that the EPS standards are in effect for US bank holding companies with total assets above US\$50 billion, firms should eschew the temptation to just meet the letter of the law and focus instead on implementing leading practices to enhance risk governance standards. By aiming high, these banks face numerous challenges (Figure 4, next page). However, they can overcome these hurdles with a combination of disciplined attention to standards and rigorous assessment of their committees’ performance.

Figure 4: Overcoming implementation challenges

Challenge 1:
Enhancing authority
and objectivity



Recommendations

- Bring all risk types into committee scope for a more comprehensive view of risk
- Create connections with other committees, but keep the risk committee in the primary oversight role for risk management
- Increase the number of independent directors on the risk committee

Challenge 2:
Building risk expertise



Recommendations

- Make sure at least one committee member has requisite risk expertise
- Educate other members on risk topics and regulatory expectations
- Ensure access to external experts

Challenge 3:
Strengthening risk reporting
and independence



Recommendations

- Formally provide for senior risk management executives' (including the CROs') unrestricted access to the risk committee
- Create incentive structures that promote sound risk management



Challenge 1: Enhancing authority

Making sure board risk committees have sufficient authority and objectivity should be a top priority, but setting the right boundaries can be difficult in practice. The analysis of board risk charters, especially those of US banks, suggests that boards have strengthened risk committee powers. However, this authority may need further extension. One such area is the ability to oversee all risk types, including emerging risks such as cyber risk, to enable the committee to develop an integrated and comprehensive view of the firm's overall risk exposure.

Overcoming the challenge: The risk committee should have, under the purview of the board, responsibility and authority to review and approve risk management policy for all risk types. Liaising with other committees

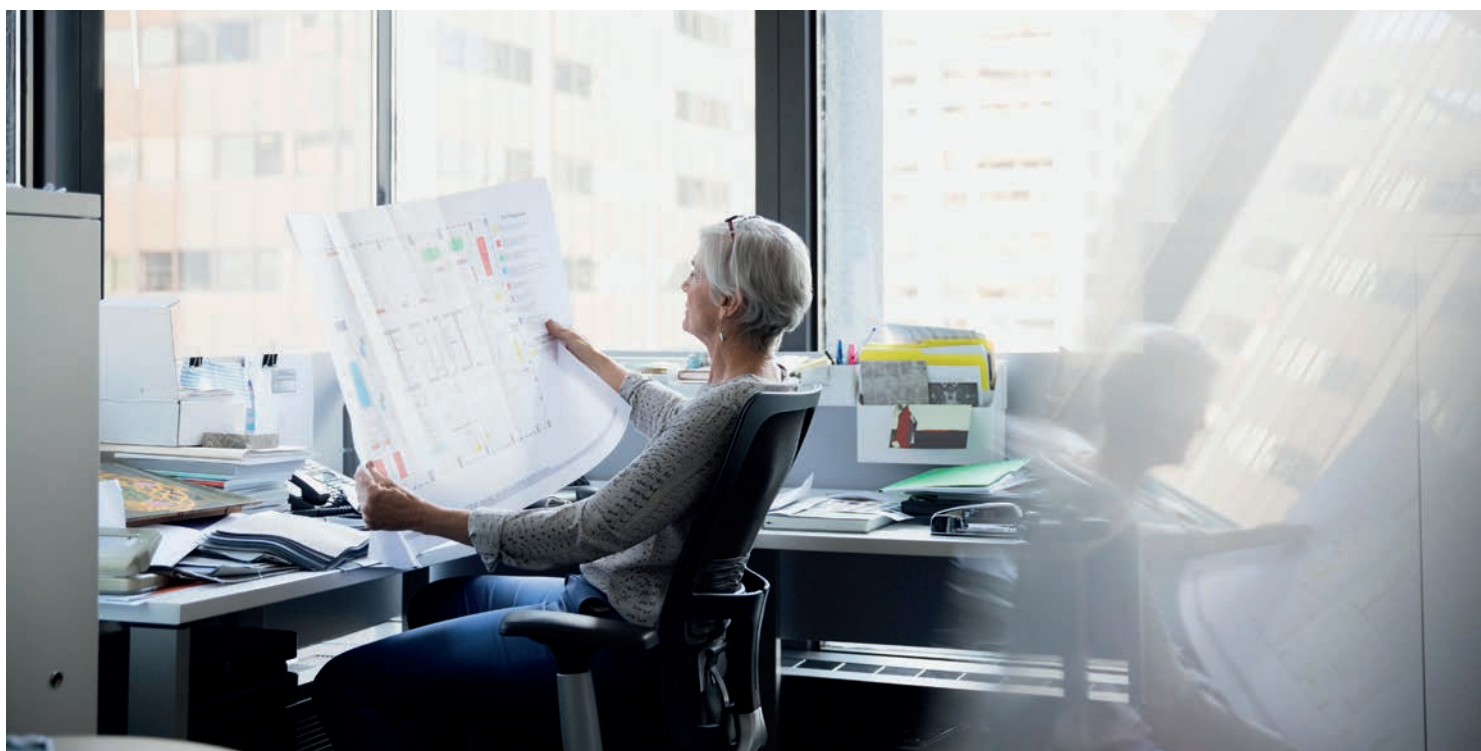
for better understanding of the firm's wider activities is helpful, even necessary, but the risk committee should be the ultimate overseer of risk policy.

An important factor in objectivity is the presence of independent directors—the Federal Reserve's EPS require the committee chair to be independent, while the OCC's Heightened Standards require two independent members. Given the importance of risk governance and the beneficial role of independent members, risk committees should seek more independent directors, and may even consider mandating a majority in their governing documents.



Challenge 2: Building risk expertise

Banks' risk exposures have grown exceedingly complex, making them steadily more difficult to understand for everyone, including experts. Accordingly, board risk committees need to continuously build the expertise



needed to fully understand the nature, extent, and potential impact of the risks that banks face.

Firms have found qualified directors with a financial background and experience in managing risks of large complex financial firms to be a limited talent pool. Additionally, many current directors may lack the technical knowledge or recent professional experience necessary to interpret quantitative risk data. This may limit their ability to form an independent view of risk and increases reliance on management's assessment.

Overcoming the challenge: Committee composition should include at least one or two risk management experts—directors who satisfy regulatory expertise requirements. Other directors should have the requisite background to understand the bank's operating environment, risk policy, and regulatory expectations. In addition, these directors also should be educated about the key quantitative parameters that the firm uses

“Board education is the biggest challenge.”

Chief Risk Officer of a G-SIB

to monitor risk and tolerance limits of those parameters, and the committee should have the authority to retain external risk and industry experts to supplement this knowledge when needed.

Cases in point: The board risk charter of ING Group explicitly requires members of the risk committee to have relevant business knowledge and adequate understanding of risk management related to the activities of the company and its group entities.⁹

⁹ Charter of the Risk Committee of ING Group N.V., ING Group Website, last updated 11 February, 2014



Challenge 3: Strengthening risk culture

Strengthened reporting structures and aligned risk and business incentives can help promote a risk-aware environment. Setting the right tone at the top is the single-most-used cliché when referring to board risk governance. However, extending responsibility and awareness of risk throughout the organization is no easy task.

Driving risk culture can be especially difficult for large organizations due to their inherent complexity. On the other hand, with regulators' eyes focused on large firms with a view to minimizing systemic risk, many smaller firms have yet to begin taking action to revamp their governance structures.

Overcoming the challenge: Fostering a strong risk culture should be as much of a board risk committee responsibility as that of senior management. Building senior management incentive structures that place a premium on being risk-aware is critical. Otherwise, governance efforts are likely to falter—with potentially serious consequences for performance.

Similarly, CROs and other senior risk personnel should have the flexibility to approach the committee at any time.

Case in point: The board risk committee charters of HSBC¹⁰ and HSBC Bank USA,¹¹ HSBC's U.S. subsidiary, provide the CRO with direct access to the committee chair at all times.

Operational burden on US BHCs of foreign banks

Many large foreign banking organizations operating in the United States will need to establish Intermediate Holding Companies (IHCs) over their US banking and non-banking subsidiaries, as part of the new EPS requirements. Essentially, these foreign banks will now need to manage their US operations as if they were standalone US bank holding companies. To transition to this new structure, foreign banks face a number of difficult tasks. They will likely need to rationalize existing entities, establish new ones, and reallocate or raise new capital to fulfill new requirements.

In particular, many foreign banking organizations will have to create new capabilities to manage risk and capital at the IHC level. The upgrades entailed as these functions are separated from the parent company will need to be designed carefully to meet the complex array of new regulatory and business needs.

Overcoming the challenge: Banks should start early to meet the new compliance requirements. Fortunately, foreign banks can take some advantage of the slightly lengthened schedules (EPS compliance by 2016, for example) to learn leading practices from domestic organizations.

¹⁰ Group Risk Committee Terms of Reference, HSBC Holdings PLC, last updated 1 August, 2014

¹¹ Risk Committee Charter, HSBC Bank USA N.A., last updated 25 July, 2014

3. Moving forward

As banks continue to revamp their risk management policies and practices, board-level risk governance should be a priority. Without careful attention to regulatory mandates and leading practices, banks may find themselves unprepared to meet ever-higher expectations. Perhaps more importantly, insufficient attention may lead to negative business consequences. As the data from our new study illustrate, many institutions have not yet shown sufficient focus.

This paper may help banks consider these crucial next moves. Our criteria and assessments indicate many basic steps toward an increasingly rigorous governance structure. Institutions that have yet to put these standards in place, or fully document them, may wish to use these as a short-term action plan.

In the longer term, however, the benefits may go beyond compliance. Some leading risk governance practices may be connected with improved performance outcomes. In an environment of continuing uncertainty and an elevated degree of regulatory risk, new investments in improved board risk governance may prove farsighted.





Global risk management survey, ninth edition - select key insights

Operating in the new normal: increased regulation and heightened expectations

Edward T. Hida II, CFA
Global Risk & Capital Management Leader
Global Financial Services Industry
Deloitte Touche Tohmatsu Limited

We are pleased to share with you here a selection of key insights from current top of mind issues explored in DTTL's Global risk management survey, ninth edition. In this feature we have selected the current issues of regulatory risk, cybersecurity and risk data and technology systems for discussion. To view the full 56-page report and the accompanying infographic, please visit <http://www2.deloitte.com/global-risk-management-survey>. For any questions regarding the survey please contact the survey editor, Edward Hida, Global Risk and Capital Management Leader, DTTL, at ehida@deloitte.com.

The global financial crisis was the catalyst for an era of sweeping regulatory change that shows little sign of abating. Across the financial services industry, regulatory requirements are becoming broader in scope and more stringent. After new regulations are enacted, it can take years before their practical implications become clear. Although the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) in the United States and Basel III were introduced several years ago, their rules are still being finalized. New regulatory developments include the US Federal Reserve's Enhanced Prudential Standards (EPS), the European Central Bank (ECB) becoming the prudential supervisor of eurozone banks, a new Banking Standards Review Council in the United Kingdom, and Solvency II becoming effective for European insurers in 2016.

The new regulatory landscape is placing demands on financial institutions in such areas as corporate governance, risk appetite, capital adequacy, stress tests, operational risk, technology data and information systems, and risk culture, to name only some areas of focus. As institutions prepare to comply, they will need the flexibility, in both their business models and compliance programs, to respond to the seemingly inevitable next round of reforms.

DTTL's *Global risk management survey, ninth edition* assesses the industry's risk management practices and challenges in this period of reexamination. The survey was conducted in the second half of 2014 and includes responses from 71 financial services institutions around the world that operate across a range of financial sectors and with aggregate assets of almost US\$18 trillion.

Key Findings

More focus on risk management by boards of directors. Reflecting increased regulatory requirements, 85 percent of respondents reported that their board of directors currently devotes more time to oversight of risk than it did two years ago. The most common board responsibilities are to approve the enterprise-level statement of risk appetite (89 percent) and review *corporate strategy for alignment with the risk profile of the organization* (80 percent).



Broad adoption of CRO position. During the course of this global risk management survey series, the existence of a Chief Risk Officer (CRO) position has grown to be nearly universal. In the current survey, 92 percent of institutions reported having a CRO or equivalent position, up from 89 percent in 2012 and 65 percent in 2002. Although it is considered a leading practice¹ for the CRO to report to the board of directors, only 46 percent of respondents said this is the case, while 68 percent said the CRO reports to the CEO.² In a positive sign, 68 percent of respondents said the CRO has primary oversight responsibility for risk management, an increase from 42 percent in 2012. Three responsibilities of the independent risk management program led by the CRO were cited by more than 90 percent of respondents: *develop and implement the risk management framework, methodologies, standards, policies, and limits; oversee risk model governance; and meet regularly with board of directors or board risk committees*. Yet only 57 percent of respondents said their risk management program had the responsibility to approve new business or products.

ERM becoming standard practice. It has become a regulatory expectation for larger institutions to have an Enterprise Risk Management (ERM) program, and this is reflected in the survey results. Ninety-two percent of respondents said their institution either had an ERM program or was in the process of implementing one, an increase from 83 percent in 2012 and 59 percent in 2008. Another positive development is that among these institutions, 78 percent have an ERM framework and/or ERM policy approved by the board of directors or a board committee.

Progress in meeting Basel III capital requirements. Eighty-nine percent of respondents at banks subject to Basel III or to equivalent regulatory requirements said their institution already meets the minimum capital ratios. The most common response to Basel III's capital requirements was to *devote more time on capital efficiency and capital allocation* (75 percent).

¹ About the term "leading practice": for the purposes of this paper, we consider industry practices to fall into a range, from leading to lagging. Some industry practices may be considered leading practices, which are generally looked upon favorably by regulators, industry professionals, and observers due to the potentially superior outcomes the practice may attain. Other approaches may be considered prevailing practices, which are seen to be widely in use. At the lower end of the range are lagging practices, which generally represent less advanced approaches and which may result in less-than-optimal outcomes. Items reflected as leading practices herein are based on survey feedback and the editor's and contributors' experience with relevant organizations

² Percentages total to more than 100 percent since respondents could make multiple selections

Increasing use of stress tests. Regulators are increasingly relying on stress tests to assess capital adequacy, and respondents said stress testing plays a variety of roles in their institutions; for instance, it enables forward-looking assessments of risk (86 percent), *feeds into capital and liquidity planning procedures* (85 percent), and *informs setting of risk tolerance* (82 percent).

Low effectiveness ratings on managing operational risk types. Roughly two-thirds of respondents felt their institution was extremely or very effective in managing the more traditional types of operational risks, such as legal (70 percent), *regulatory/compliance* (67 percent), and *tax* (66 percent). Fewer respondents felt their institution was extremely or very effective when it came to other operational risk types such as third party (44 percent), *cybersecurity* (42 percent), *data integrity* (40 percent), and *model* (37 percent).

More attention needed on conduct risk and risk culture. There has been increased focus on the steps that institutions can take to manage conduct risk and to create a risk culture that encourages employees to follow ethical practices and assume an appropriate level of risk, but more work appears to be needed in this area. Sixty percent of respondents said their board of directors works to *establish and embed the risk culture of the enterprise and promote open discussions regarding risk*, and a similar percentage said that one of the board's responsibilities is to review incentive compensation plans to consider alignment of risks with rewards, while the remaining respondents said these were not among the board's responsibilities. Only about half of respondents said it was a responsibility of their institution's risk management program to review the compensation plan to assess its impact on risk appetite and culture.

Increasing importance and cost of regulatory requirements. When asked which risk types would increase the most in importance for their institution over the next two years, regulatory/compliance risk was most often ranked among the top three, and 79 percent felt that *increasing regulatory requirements and expectations* were their greatest challenge. The most important impact of regulatory reform was *noticing an increased cost of compliance*, cited by 87 percent of respondents.



A closer look at select current issues

Regulatory risk

The wave of change since the global financial crisis has constituted the most far-reaching revision of regulatory requirements in decades, significantly increasing compliance requirements. The era of regulatory reform is far from over, with additional proposals from the Basel Committee and with final rules still to be established for many provisions of the Dodd-Frank Act in the United States and for the CMU and the EU regulations and directives in Europe.

The impacts of these more-stringent regulatory requirements are significant for many institutions, including higher capital requirements, restrictions on business activities, additional documentation for regulators, and new standards on risk data and infrastructure. Regulators are also turning their attention to qualitative issues, such as risk culture and the effectiveness of internal controls.

One result of all these regulatory requirements has been increased costs. When asked about the impacts of regulatory reform on their institution, respondents most often mentioned noticing an increased cost of compliance (87 percent up from 65 percent in 2012). Other impacts cited often were maintaining higher capital (62 percent up from 54 percent in 2012) and adjusting certain products, lines, and/or business activities (60 percent up from 48 percent).

Many respondents are concerned that compliance costs will continue to escalate. Considering the potential impact on their organization of supervisory and regulatory processes, respondents were most often extremely or very concerned about issues related to cost: *tighter standards or regulations that will raise the cost of doing existing business* (72 percent) and *growing cost of required documentation and evidence of program compliance* (60 percent).

The impacts of examinations and enforcement actions were also mentioned by many respondents: *regulators' increasing inclination to take formal and informal enforcement actions* (53 percent) and *more intrusive and intense examinations* (49 percent).

New regulatory requirements have not only increased costs, they have also limited the ability of many institutions to generate revenues. Reflecting this new reality, 43 percent of respondents said they were extremely or very concerned about *new restrictions or prohibitions on profitable activities that will require a significant change in business model or legal structure*.

Cybersecurity

Cybersecurity is an operational risk type that has become a high priority for financial institutions and regulators. The number and extent of cyber-attacks have shown "exponential growth"³ according to one corporate security chief, with the financial services industry as a top target.⁴ In response, double-digit increases in bank security budgets are expected in the next two years.⁵ Once seen as only an IT issue, the impacts of cyber-attacks can spread across the organization and affect business lines, operations, legal, and communications, among other areas. With their widespread impacts, cybersecurity events also pose significant reputational risks to a company.

With the increase of major hacking incidents from both criminal enterprises and potentially state-sponsored actors, cybersecurity has been a major focus for regulators. In February 2015, the SEC's Office of Compliance Inspections and Examinations released the results of its examinations in 2014 of cybersecurity practices at more than 100 registered broker-dealers and investment advisers.⁶ In the same month,



FINRA published its recommendations on effective cybersecurity practices, based on its 2014 examinations of financial services firms.⁷ FINRA has announced that cybersecurity will again be one of its examination priorities in 2015.⁸

Given the increasing regulatory requirements and the potential reputational damage that can result from a data breach, financial institutions need a comprehensive cybersecurity program. Among the leading practices for such a program are that it places a priority on threats with the greatest potential impact and on safeguarding sensitive data and critical infrastructure; it implements a formal written plan to respond to cybersecurity incidents; it conducts penetration testing; has dedicated personnel; and it periodically reviews the firm's cyber insurance strategy.

42 percent of respondents felt their institution is extremely or very effective in managing cybersecurity, roughly similar to the percentage of respondents that said the same about managing third-party risk (44 percent). Third-party and cybersecurity risk are sometimes closely related since there have been security breaches involving third parties that have affected the confidentiality of customer information.

Respondents at large institutions (63 percent), which have more resources to devote to safeguarding their data and information systems, were more likely to consider their organization to be extremely or very effective in this area than those at mid-size (35 percent) or small institutions (25 percent).



Risk data and technology systems

The global financial crisis underscored the need for risk data that are accurate, timely, consistent, and aggregated across the enterprise. Since then, risk data has been a priority for regulators.

In 2013, the Basel Committee issued its BCBS 239 paper, which emphasizes that banks need systems capable of producing aggregated risk data for all critical risks during times of stress or crisis.⁹ Banks must also fully document and validate their aggregation capabilities and reporting practices. G-SIBs must comply by 1 January 2016, and BCBS 239 suggests that supervisors apply the same rules to domestic systemically important banks (D-SIBs).

CCAR's stress tests require banks to aggregate risk data across regions and lines of business.¹⁰ There are also stricter requirements for data quality and aggregation in various capital and liquidity requirements, Solvency II, the OCC's heightened standards, and MiFIR, among other regulations.

Complying with these requirements is an arduous task for some institutions. For example, many eurozone banks encountered difficulties in providing the accurate, timely data required by the ECB's asset quality review.¹¹ When asked about the challenges facing their institution, many respondents said that *risk information systems and technology infrastructure* (62 percent) and *risk data* (46 percent) are extremely or very challenging.

3 Vikram Bhat and Lincy Francis Therattil, "Transforming cybersecurity: New approaches for an evolving threat landscape," Deloitte LLP, 2014, <http://www2.deloitte.com/us/en/pages/financial-services/articles/dcfcs-transforming-cybersecurity.html>

4 Mandiant, "Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry," 23 September 2013, as cited in Deloitte US's infographic "Transforming cybersecurity: New approaches for an evolving threat landscape"

5 Daniel Huang, Emily Glazer, and Danny Yadron, "Financial Firms Bolster Cybersecurity Budgets," Wall Street Journal, 17 November 2014, <http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536>

6 "Cybersecurity Examination Sweep Summary," Office of Compliance Inspections and Examinations, Securities and Exchange Commission, 3 February 2015, <http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf>

7 "SEC and FINRA Issue Results of Cybersecurity Examinations," The National Law Review, 18 February 2015, <http://www.natlawreview.com/article/sec-and-finra-issue-results-cybersecurity-examinations>

8 "2015 Regulatory and Examination Priorities Letter," Financial Industry Regulatory Authority, 6 January 2015, <https://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p602239.pdf>

9 "From principles to practicalities: Addressing Basel risk data aggregation and reporting requirements," Deloitte US, 2013, <http://www2.deloitte.com/us/en/pages/regulatory/basel-risk-data-aggregation-and-reporting-requirements.html?nc=1>

10 Joe RENNISON, "Stress, tested," Risk Magazine, August 2014

11 "Top 10 for 2015: Our outlook for financial markets regulation," Deloitte EMEA Centre for Regulatory Strategy, 2015, <http://www2.deloitte.com/global/en/pages/financial-services/articles/regulatory-top-ten-for-2015.html>

In response to these stricter requirements, many financial institutions have undertaken major data remediation and infrastructure programs. Progress has been made, but significant work remains to be done at many institutions.

Less than half of the respondents rated their institution as extremely or very effective in any area of risk data and infrastructure, although the ratings improved since 2012: *data management/maintenance* (39 percent compared with 20 percent in 2012), *data process architecture/workflow logic* (35 percent compared with 23 percent), and *data controls/checks* (31 percent roughly similar to 33 percent in 2012).

The pace of regulatory change places additional demands on risk technology systems. 48 percent of respondents said they are extremely or very concerned about *risk technology adaptability to changing regulatory requirements*, an increase from 40 percent in 2012, while 46 percent of respondents said the same about lack of integration among systems, up from 31 percent in 2012.

Most of the survey participants are multinational institutions, with 68 percent having operations outside their home country



About the survey

The full report presents the key findings from the ninth edition of Deloitte's ongoing assessment of risk management practices in the global financial services industry. The survey gathered the views of CROs or their equivalents at 71 financial services institutions around the world and was conducted from August to November 2014.

The institutions participating in the survey represent the major economic regions of the world, with most institutions headquartered in the United States/Canada, Europe, or Asia Pacific (Figure 1). Most of the survey participants are multinational institutions, with 68 percent having operations outside their home country. The survey participant companies provide a range of financial services offerings, including insurance (58 percent), banking (55 percent), and investment management (48 percent) (Figure 2).¹²

The institutions have total combined assets of US\$17.8 trillion and represent a range of asset sizes (Figure 3). The survey participants that provide asset management services represent a total of US\$5.6 trillion in assets under management.

Where relevant, the report compares the results from the current survey with those from earlier surveys in this ongoing series. Deloitte's *Global risk management survey* is conducted biennially.

Analysis by asset size

In this report, selected survey results are analyzed by the asset size of participating institutions using the following definitions:

- Small institutions - Institutions with total assets of less than US\$10 billion
- Mid-size institutions - Institutions with total assets of US\$10 billion to less than US\$100 billion
- Large institutions - Institutions with total assets of US\$100 billion or more

¹² Percentages total to more than 100 percent since some institutions provide more than one type of service. In the report, institutions that provide insurance services will sometimes be termed "Insurers" (even if they also provide other types of financial services) and institutions that provide investment management services will sometimes be termed "investment management companies" (even if they also provide other types of financial services)

Figure 1: Participants by location of headquarters

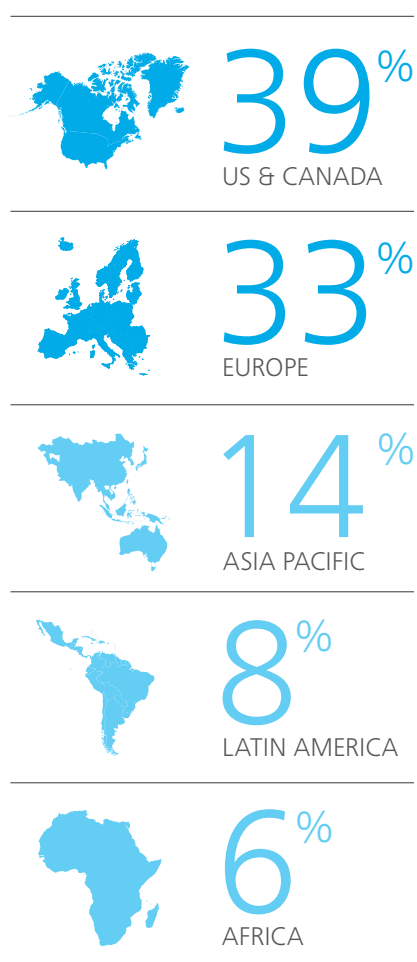
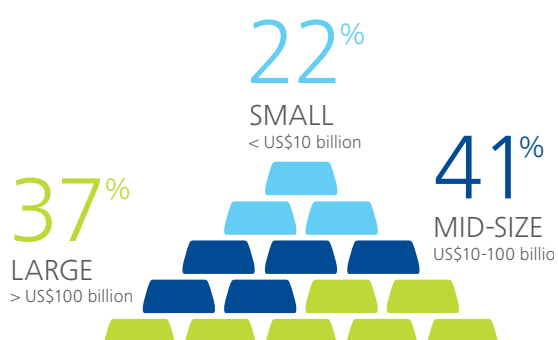


Figure 2: Participants by financial services provided



Figure 3: Participants by asset size



Note: percentages do not total 100% since respondents could make multiple selections.



Conclusion

The era of regulatory reform sparked by the global financial crisis has become the new normal. There have been an ongoing series of new regulations affecting risk governance, capital adequacy, liquidity, stress testing, and prohibitions on proprietary trading, among other areas. Institutions are being required to enhance their capabilities for managing operational risk, with both regulators and management especially concerned about the impacts of hacking and other types of cyber-attacks. Regulators are also focusing on the qualitative aspects of risk management. They are looking beyond quantitative measures of market, credit, and liquidity risk to assess whether institutions have created a culture that encourages employees to take appropriate risks and that promotes ethical behavior more broadly. In this effort, it is essential that incentive compensation schemes are aligned with an institution's risk appetite.

Success in all these areas depends on quality risk data and effective information systems. Yet, developing accurate, aggregated risk data on a timely basis remains a challenge. Measurement can be especially difficult for some risk types, such as operational risk, and for qualitative issues, such as risk culture. DTTL's Global risk management survey indicates there has been progress in many of these areas. But with the regulatory expectations being ratcheted up continually, institutions will need to keep pace by regularly upgrading their risk management capabilities:

- Many institutions have implemented strong risk governance at the level of their board of directors and senior management, including implementing an ERM program and creating a CRO position. They will now need to broaden their perspective to consider how they can manage conduct risk by embedding a risk culture throughout their organization that encourages ethical behavior by employees. Keys to this effort will be the board of

directors and senior management communicating the value the organization places on treating customers fairly and also having incentive compensation practices that reward ethical behavior and appropriate risk-taking

- As regulators rely more on stress tests to assess capital adequacy and liquidity, institutions will need to improve their stress-testing capabilities and attract personnel with the required skills and experience. The talent shortage noted in the survey will make this an ongoing challenge
- More effective management of operational risks, especially cybersecurity, will be essential. Institutions will not only need to improve their IT security processes, but also their processes for selecting vendors and assessing their security procedures
- Institutions will need to reassess their risk data and information systems. Many institutions will need to improve their access to high-quality and timely risk data as well as their ability to quickly aggregate risk data across lines of business and geographies

Financial institutions are adjusting to the new environment for risk management. Most institutions will need to enhance their risk management programs to stay current—improving analytical capabilities, investing in risk data and information systems, attracting risk management talent, fostering an ethical culture, and aligning incentive compensation practices with risk appetite. They will find that business strategies and models must be reassessed in response to changed regulations more often than before. Perhaps most important, institutions will need to develop the flexibility to respond nimbly to the “new normal” risk management environment of unceasing regulatory change.



The era of regulatory reform sparked
by the global financial crisis has
become the new normal

To view the full 56-page report and the accompanying infographic, please visit <http://www2.deloitte.com/global-risk-management-survey>.

What are they saying?

New ways to detect emerging reputation (and other strategic) risks

Henry Ristuccia

Global Governance, Regulatory & Risk Leader
Deloitte Touche Tohmatsu Limited

Peter Dent

Global Crisis Management Leader
Deloitte Touche Tohmatsu Limited

Reputation risk often tops the list of those that keep senior executives and board members up at night. That concern is not misplaced. Reputation risk emanates from financial, operating, security, compliance, legal, and other risk events, and when those events come to light, that light can be harsh.

This is particularly the case in the social media and virtual worlds, where incidents and decisions that would escape notice or comment a mere five years ago, now find a global audience ready to take organizations to task within hours and often with serious repercussions.

Not incidentally, reputation risk usually falls outside traditional risk management frameworks and Enterprise Risk Management (ERM) capabilities. Yet reputation risk must be proactively managed as a risk given its ability to damage brands, lines of business, and entire organizations. Indeed, this elevates reputation risk to the level of strategic risks, which means it warrants senior executive and board-level attention.

As with most risks, the sooner reputation risk is recognized and addressed, the better. Yet approaches to managing reputation risk tend to focus mainly on cultivating a good reputation and countering setbacks through effective communication. While essential, these activities are no longer enough, given that reputation risk can emerge so quickly and from so many directions. Management therefore needs explicit means of recognizing the potential reputational impact of an incident or decision and of proactively addressing reputation risk.

The right capabilities, enabled by innovative technologies, can position the organization to identify, detect, track, mitigate, and manage reputation risk—and other strategic risks—more proactively than traditional capabilities and reactive communication. Indeed, many companies are seeking better methods of addressing reputation risk, and working to apply them.



¹ 2014 global survey on reputation risk: Reputation@Risk, October 2014, Deloitte <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf>

Reputation risk = Strategic risk

Reputation risk is unique in that almost any other risk can—when significant enough—generate reputation risk. Social media and the virtual world have lowered the threshold of significance such that minor incidents or seemingly innocuous decisions (or statements) can damage reputation, unless they are handled well. In addition to financial, operating, security, compliance, and legal risks, risks related to conduct, ethics, and integrity, corporate responsibility and sustainability, and products, services, and customer sentiment can drive reputation risk. Any of these risks within a third-party relationship can also expose an organization to reputation risk.

Reputation risk is a strategic risk in that it can undermine the organization's ability to implement strategies or achieve strategic goals. That is why reputation risk topped the list of strategic risks cited by respondents in the 2014 Reputation@Risk survey¹, conducted by Forbes Insights on behalf of Deloitte Touche Tohmatsu Limited (DTTL).

Reputation risk is unique in that almost any other risk can—when significant enough—generate reputation risk

That survey of more than 300 executives from companies in every major industry and geographic region found that companies are investing in capabilities for managing reputation risk. More than half (57 percent) plan to invest in related data, analytical, and brand-tracking tools, including media/negative-mention monitoring, social media monitoring, and surveys. Yet respondents in that survey cited the key drivers of reputation risk as relating to ethics and integrity, including fraud, bribery, and corruption (55 percent), followed by physical and cyber security risks (45 percent), and product and service risks (43 percent).

These top three drivers—ethics and integrity, physical and cyber security, and product and service risks—matched those identified by companies that had actually experienced a major reputation risk event. Furthermore, respondents expected these drivers to top the list for at least the next three years. Third-party relationships are another key risk area, as companies are increasingly being held accountable for the suppliers' and vendors' actions. These findings may indicate that organizations should cast a broader net when monitoring reputation risk.

A strategic risk-sensing program provides that broader net. It also provides decision-makers with real-time awareness of events that are likely to affect reputation. Such a program extends beyond news media, social media, and customer sentiment monitoring to identify a wide range of emerging risks early enough for management to head them off or mitigate them. Most leading organizations have some sort of program designed to detect and track emerging risks. However, the purpose, shape, and implementation of these programs vary widely.

¹ 2014 global survey on reputation risk: Reputation@Risk, October 2014, Deloitte <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf>

Defining risk sensing

On the basis of ongoing work, Deloitte has developed a definition of risk sensing, as well as related concepts, practices, and capabilities. In general, risk sensing uses advanced technologies to selectively scan and analyze the internet and social media for structured and unstructured facts, figures, reports, and opinions for specific emerging risks, risk indicators, and potential risk events. The goal is to detect and track nascent risk events and anomalous data in order to monitor changes, trends, and patterns, and to distill the results into actionable information.

Strategic risk sensing aims to identify, analyze, and monitor emerging risks that could impact reputation as well as other strategic risks to the organization. Advanced analytics, combined with selected risk indicators, enable analysis of data against benchmarks and across potential scenarios with the aim of identifying risks most relevant to the organization's senior executives and decision-makers. Sophisticated scanning and analysis also identifies emerging trends outside the defined risk universe that could eventually impact reputation.

A robust risk-sensing capability encompasses the following characteristics:

Strategic focus

Most major organizations monitor financial, operational, compliance, and other risks to the business. Additional risk-sensing opportunities arise from identifying strategic risks—those that could undermine achievement of strategic goals, negate management's assumptions, or exceed the organization's risk appetite.

Senior executive engagement

Senior executives should ensure that risk sensing remains relevant and is integrated into the risk governance and risk management program. Their involvement should also preclude siloed approaches to risk sensing.

Outside-in points of view

External analysts who understand the organization's goals and risks can often provide more forward-looking, objective views than internal parties. Their views can also correct for the internal biases of management and staff analysts.

Listening posts

Listening posts enable tracking of trends in social media and news sources, such as changes in customer sentiment. Listening posts can also be established to monitor changes in employee sentiment, regulatory expectations, and other specific patterns and trends.

Metrics and tracking

Real-time risk indicators enable monitoring of risks against objective baseline measures and thresholds. A risk-sensing program should also include early warnings and triggers (relative to risk tolerances) for evaluating, communicating, and mitigating risks.

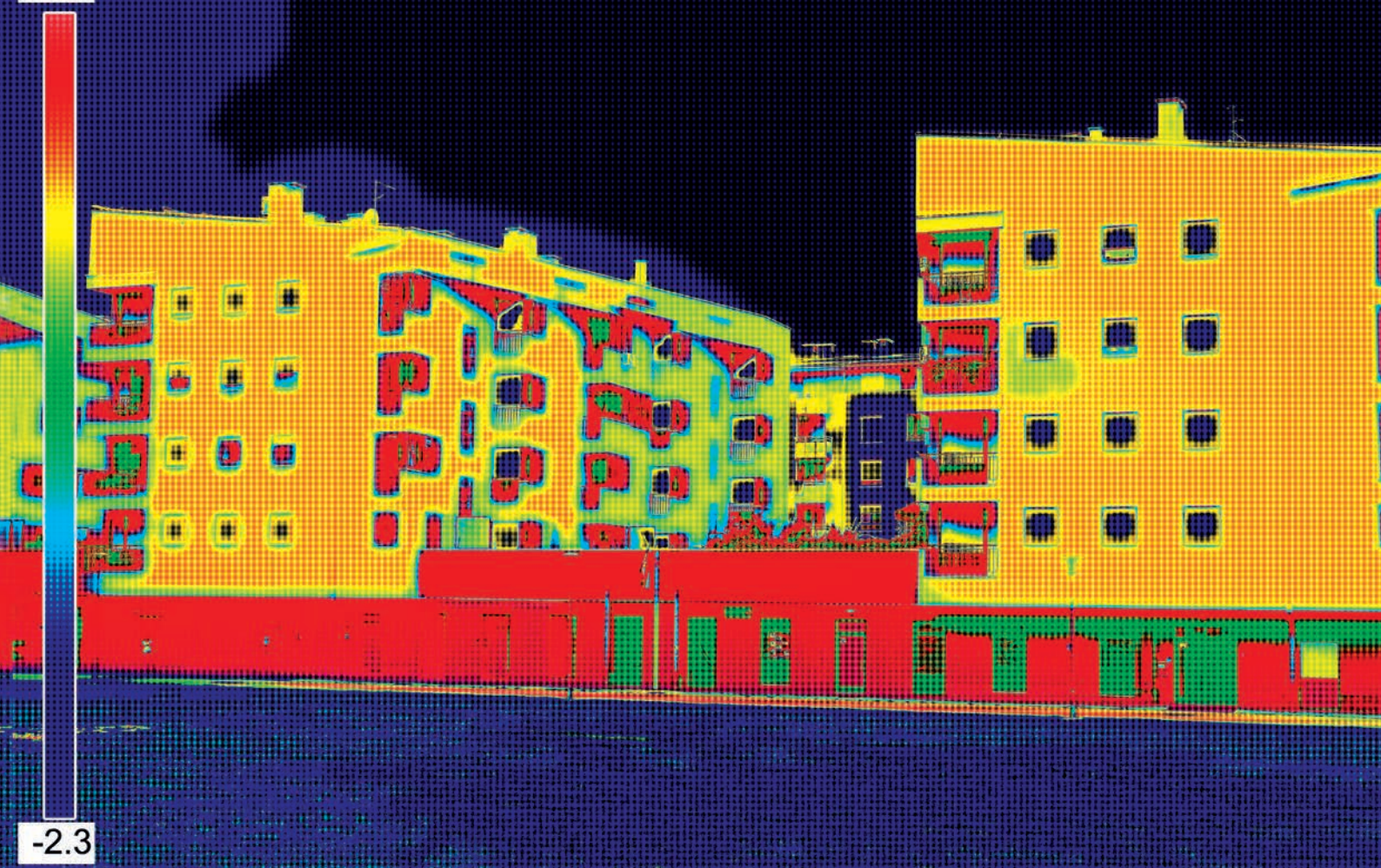
Combined technological and human resources

Analyzing and predicting rare and nascent events has become increasingly possible with advances in text and data analytics. Yet human analysis enriches these views and provides valuable, otherwise unavailable insights.

Rather than reams of data, decision-makers need summary reports, concise insights, and visualization tools such as dashboards. Risk sensing should not be the domain of isolated specialists or technologists. A direct line from the sensing team and the CRO to the CEO and board would be useful, particularly for communicating emerging strategic risks.

Variations among companies' risk-sensing efforts are to be expected, given that risk sensing is relatively new and organizations must adapt it to their needs. Specialized efforts, such as those for detecting changes in customer sentiment, political risk, credit risk, or compliance risk, remain useful. Yet the range of today's risks argues for broad, deep, truly strategic risk-sensing programs. Although the technology and expertise is available, such programs depend on innovative but rigorous application of those resources.

19.3



An application of risk sensing

Deloitte uses 24/7 monitoring itself to integrate certain monitoring capabilities into an intelligence platform for filtering and correlating data from social media, news feeds, financial reports, and government agency announcements—among other sources. These capabilities can also be used to monitor post-event impacts, such as effects of a weather-related event on the supply chain of key clients or the reputational impact of cyber incidents.

The 24/7 monitoring methodology addresses risks in five areas: cyber, communications, geopolitical events and man-made or natural disasters, financial crime, and distressed entities. For example, the methodology can be applied in the following areas and ways:

- **Cyber:** malware and data monitoring, cyber watch analysis, confidential and personal data monitoring, targeted vulnerability monitoring
- **Communications:** social and traditional media monitoring, reputation and brand monitoring, privacy and public relations monitoring, industry and competitive intelligence
- **Geopolitical/disasters:** business risk analysis, risks to human resources and infrastructure, real-time disaster and supply chain risk analysis, post-incident resilience and crisis management

Depending on the nature of the threat, this capability can integrate internal data generated by the organization with data from external sources. Automated monitoring detects events, trends, and anomalous data more efficiently and effectively than human analysts; however, human analysts apply experience and judgment to understand the organizational implications of the output.

This capability transforms data into actionable information delivered via an interactive customized dashboard. The dashboard provides both text and graphic incident reports in summary form by category of threat, and monitors the severity and status of the threat.

24/7 monitoring is just one of many forms risk sensing may take. Regardless of the specific form, success depends on the ability of internal and external team members to identify risks to the organization, indicators of those risks, and sources of relevant data—and then to design and implement a platform to monitor all three, and to act on the output.

A look at risk-sensing practices

A DTTL/Forbes Insight risk-sensing survey held in May/June 2015² indicates that most large organizations are engaged in risk sensing as they define it. The survey findings—and Deloitte’s experience in the field—indicate that risk-sensing efforts are subject to different definitions and are often missing elements that could benefit the organization.

For example, a program may focus on a narrow set of risks, reside in an isolated technical or business unit, or omit other characteristics of a strategic risk-sensing program. As would be expected, organizations also vary in the risks they monitor, the positions to which risk sensing efforts report, and the risks they view as important.

The following are among the key findings of the DTTL/Forbes Insight risk sensing survey:



Companies apply risk sensing, but less often to strategic risks

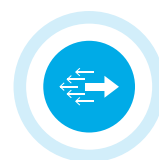
About 80 percent of respondents agree that they use risk sensing tools. However, based on the top three “Agree” answers on a scale of 1 to 10, they apply them most often to financial risk (71 percent), compliance risk (66 percent), and operational risk (65 percent), and less often to strategic risk (57 percent). Yet strategic risks tend to be most important to senior executives and the board.



Management’s perceptions of risks shift slowly

A similar DTTL/Forbes Insights survey carried out in 2013³ asked respondents to choose the major strategic risks they faced three years prior, at the time of the survey, and three years ahead, as did our 2015 survey. The more recent survey shows that perceptions of risks have shifted somewhat.

- Reputation risk remains among the top three in all three timeframes in the 2013 and 2015 surveys, while economic trends diminish as a concern in 2015. In the 2015 survey, regulatory risk joins reputation risk as a concern in all three timeframes. The pace of innovation stands among the top three risks in 2015 and (in a tie with regulatory risk) tops the list in 2018. These findings indicate that management’s views of risks shift, though not quickly. It is therefore useful to define risks broadly, because management’s definitions of risk tend to direct risk-sensing efforts. Also, risks rarely remain static, which underscores the need for external viewpoints to provide broader perspective and greater objectivity.



External points of view may be undervalued

Many respondents agree that outside parties have more objectivity about risks than insiders, but even more do not agree. A total of 40 percent “Agree” (as measured by the top three levels of agreement), yet those in the middle range (4 through 7 on a ten point scale) total 51 percent, indicating uncertainty about the value of external viewpoints. This finding may be skewed by respondents who consider external views as including—or consisting of—social media or reviews and ratings on websites, which they may devalue.

- Meanwhile, 10 percent disagree or disagree completely that an outside perspective can analyze risks with greater objectivity. This could indicate strong, potentially dangerous internal biases. External points of view can be particularly useful for weighing risks regarding reputation and the pace of innovation. Organizations can underestimate risks to reputation by overweighting positive customer survey results and dismissing negative views. On innovation, major companies often see new technologies as immature or irrelevant only to find themselves battling new competitors with disruptive business models sooner than they ever thought possible.

A Deloitte/Forbes Insight risk-sensing survey held in May/June 2015² indicates that most large organizations are engaged in risk sensing as they define it

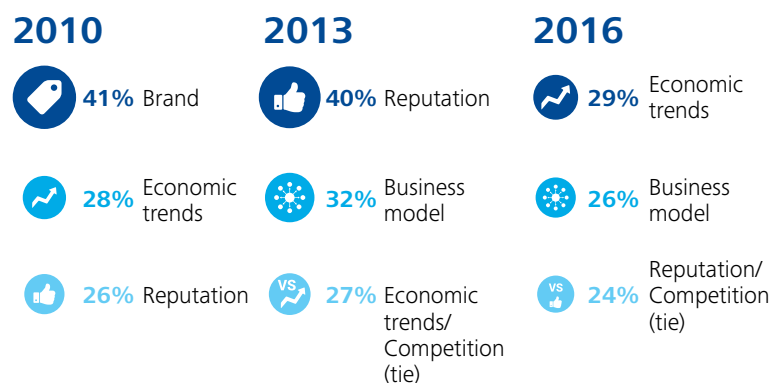


Two-thirds believe they have the right people

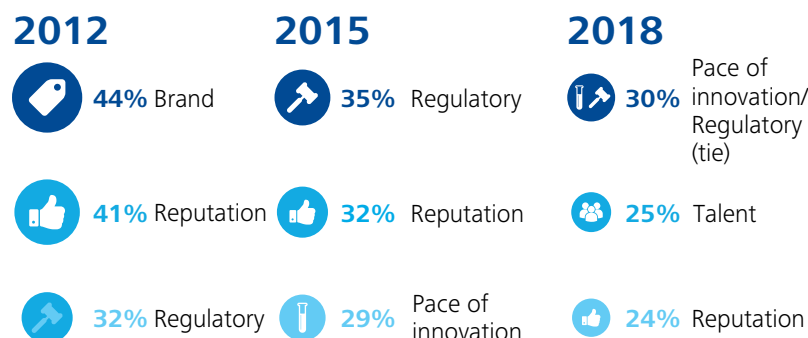
Two-thirds of respondents agree (based on the top three “Agree” responses) that they employ people with the knowledge needed to monitor, analyze, and act on risk-sensing data. One-third are less certain. The largest companies in the survey—those with at least US\$5 billion in annual revenue (as opposed to those in the US\$1 billion to US\$5 billion range)—most often agree, as may be expected given their deeper talent pool.

- When the risk-sensing team is large, respondents’ answers could indicate that the company relies more on people than on technology. While some companies use visualization tools and dashboards, fewer use pattern analysis, scenario analysis, or other leading-edge analytics. The right tools reduce initial data gathering and analysis and free human resources for higher value-added activities.

Risks of most concern in 2013



Risks of most concern in 2015



² Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing, DTTL, 2013 <<http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-exploring-strategic-risk.pdf>>

³ Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing, DTTL, 2013 <<http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-exploring-strategic-risk.pdf>>

Getting risk sensing right

Forward-looking organizations are linking strategy development and risk assessment more closely. While many companies have long done this, efforts have often been siloed and thus disconnected. As a result, data on risks and opportunities often goes undetected or fails to make it upstream or to other relevant parties. Meanwhile, data on the next devastating risk or golden opportunity usually already exists within the organization or in cyberspace. Yet no one links that data to the strategic assumption or driver of value that may be (or will be) affected.

A starting point would be for the organization to identify the factors that, if negatively impacted, would alter the forces that drive the organization's sector. Those forces can be organized into domains, such as economic, regulatory, customer, technological, operational, and research and development, and include scientific, engineering, or other advances that could affect drivers of value.

Within specific domains, certain data will reflect existing and potential events and trends related to the sector or organization.

Consider, for example, the following sample issues and themes within each of these common domains:



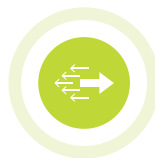
Economic

Regional and national growth, interest rate and currency environments, sector developments, input costs (including labor), supply and demand dynamics



Regulatory

Legislative developments, regulatory agency priorities, compliance methods and costs, case law and litigation trends



Customer

Product and service preferences, factors influencing purchase, evolving customer journey, competitive product and pricing strategies, technology adoption curve



Technology

Basic science and R&D trends, knowledge transfer, technology commercialization, academic activity, patent filings and citations, technology acquisitions



Operational

Supply chain, alternate suppliers, capacity issues, production and delivery challenges, outsourcing, use of alliances and channel partners



These are sample domains and issues. Actual domains and issues would be specific to the organization and its sector. Also, domains overlap in ways that must be identified so interactions among them can be mapped to risks and opportunities.

Four steps to implementation

Developing, launching, and maintaining a risk sensing program requires dedicated resources, starting with internal people who understand the company's business and unique risks. External resources may also be required, given the need for a technology platform, sophisticated analytics, and outside-in perspectives. Risk sensing also requires the expertise of data scientists, data engineers, and sector analysts to identify required data and data sources, define optimal workflows, and develop formats for dashboards and reports. Here are four steps to consider when framing and implementing a strategic risk scanning, sensing, and tracking program:

1 Identify the strategic risks to be monitored, and the scope of the effort

Senior leaders and key stakeholders can begin by identifying and prioritizing strategic risks, and agreeing on the risks, domains, and potential disruptors to be monitored. The scope of the effort will be determined by the risks to be monitored, the metrics to be tracked, and the thresholds that will trigger communication, escalation, and countermeasures. Management should define the scope as strategic and enterprise-wide.

2 Define the elements required to enable strategic risk monitoring

The team can then identify the technology and human resources required for the program, which will depend on the risks and data sources to be monitored and desired data extracts and reports. The team must identify the outputs—the data, analyses, flags, and insights—and the visualization tools best suited to representing them. This step should also define the workflows required to analyze the risks, generate the output, and communicate and act upon the results.

3 Configure the platform to enable scanning, sensing, and tracking of risks

After the workflows are structured and the supporting technology and human resources are in place, scanning, monitoring, data extraction, and analysis begin. Initial output is reviewed and early insights are developed. The data and findings can be enriched with sector, economic, marketplace, regulatory, and other information, and the initial results fine-tuned.

4 Continue monitoring the data sources and generating ongoing insights

The team, working with senior executives, risk managers, and other stakeholders, continues to develop insights regarding strategic risks and issues. Users of the output must incorporate the insights into key plans and decisions such as those related to product development and discontinuation, market initiatives, IT purchases, human resource allocation, and mergers and acquisitions. If this is not happening, everyone must learn why—and decide how to make it happen.

The team must continue to sharpen the scanning and analysis, expand or narrow the program's scope, improve dashboards and reports, and deepen the information and insights. Perhaps with external assistance, the team should periodically review and validate the program, considering its scope, practices, resources, and output and then revise elements accordingly.

In terms of the team, in addition to senior executives, business unit leaders, and risk managers, the following individuals would be useful in developing and refining a risk-sensing program:



Specialists

Individuals with expertise in analytic methods, such as developers of process modules



Platform sector analysts

Analysts working with specialists to develop the sector analysis and to define required workflows



Dedicated analysts

Analysts who use the platform, with guidance from sector analysts and specialists, to refine specific reports and reporting mechanisms

The combined technological and human resources give risk sensing its detection and analytical powers. The tools and the people are critical to success.

A risk management essential

These days, seemingly insignificant issues can become global headlines that undermine hard-won reputations. Leading organizations already treat reputation risk as a strategic issue, a trend that should accelerate. Unfortunately, many companies are underprepared to manage reputation risk.

Risk sensing can help in detecting emerging issues, but the right capabilities must be in place before a crisis hits. A true strategic risk-sensing program goes beyond tracking a handful of risks and specific risk indicators in several media. Rather, it identifies a broad range of reputational, strategic, and other risks to the organization, scans myriad sources of data and information, and leverages technological and human resources optimally. It also produces output of high value to senior-level decision-makers.

Recent D TTL/Forbes Insight surveys indicate that most large organizations have risk-sensing efforts underway, but that many may have a way to go if those efforts are to become true risk-sensing programs. In general, the value of an organization's program will reflect the extent to which it is tied to strategic risks and priorities, supported by senior executives, integrated with risk governance and risk management, and comprised of the right resources.

Not incidentally, Deloitte has embedded risk-sensing technology in its own risk governance structure to promote understanding of how brand-impacting events might affect the organization, and to enable adjustments to strategies.



Risk sensing A tool to address reputation risks

Henry Ristuccia
Partner
Deloitte US

Chuck Saia
Partner
Deloitte US

Reputation risks are driven by a host of other business risks—particularly those in the areas of ethics and integrity; security; and products and services—with third-party relationships rapidly emerging as a critical risk area, according to the 2014 Reputation@Risk survey conducted by Forbes Insights on behalf of Deloitte Touche Tohmatsu Limited (DTTL).

The survey, which reflects the views of more than 300 executives from companies representing every major industry and geographic region, found that companies are investing to improve their capabilities for managing reputation risk. More than half (57 percent) of the companies surveyed plan to address reputation risk by investing in technology, such as analytical and brand monitoring tools, to help strengthen their risk-sensing capabilities. They also plan to invest in data, including traditional media/negative-mention monitoring, social media data, surveying, and other data sources.

Henry Ristuccia

Risk sensing provides executive-level decision-makers with real-time market awareness on issues that are likely to affect a company's reputation. *"Risk sensing is especially important because it can help the organization to identify emerging problems while there is still time to head them off,"* says Henry Ristuccia, a partner with Deloitte & Touche LLP. *"This is what a truly effective approach to managing reputation risk requires: constant vigilance—before, during and after a crisis."*

Integrating risk-sensing capabilities and technologies into a company's day-to-day business processes can provide decision-makers with the deep and timely insights they need to address potential problems before they turn into crises.

These capabilities may include:

Real time: Efficiently processing and synthesizing real-time intelligence, such as pattern detection and recognition, for real-time reporting

Text analytics: Using natural language processing, sentiment analysis, and computational linguistics to identify and extract subjective information from structured and unstructured data sources

Big data: Cost-effectively monitoring internal and external data

Forward-looking: Taking an outside-in view to supplement findings and assessing strategic, operational, and tactical business drivers in the future

Early warning and triggers: Increasing signal-to-noise ratio to detect weak and early warning signals and avoid surprises

Actionable insight: Operational insights that can be easily integrated and can have a direct positive effect on the business

Chuck Saia

"While risk sensing can help identify emerging problems, all of the capabilities need to be in place before a crisis hits—because the absolute worst time to develop a crisis management strategy is when your back is against the wall and you're running out of options," says Chuck Saia, Chief Risk, Reputation and Regulatory Affairs Officer for Deloitte LLP in the United States, who also serves as Reputation and Crisis Leader.

"At Deloitte, we have embedded risk-sensing technology in our governing structure so we can understand how brand-impacting events affect organizations like ours, allowing us to adjust our strategies," he adds.

Reputation@Risk Survey highlights

The top underlying drivers of reputation risk were found to be related to ethics and integrity (55 percent), such as fraud, bribery, and corruption; followed by security risks (45 percent), both physical and cyber; and product and service risks (43 percent). These three drivers are expected to remain the leading factors for at least the next three years. Third-party relationships are another rapidly emerging risk area, as companies are increasingly being held accountable for the actions of their suppliers and vendors.

The top three drivers of reputation risk today are the same as the top drivers identified by companies that experienced a major reputation risk event in the past, according to the survey. Furthermore, these same drivers are expected to remain at the top of the list for at least the next three years.

Other findings

- Reputation problems have the biggest impact on revenue and brand value. Respondents who had previously experienced a negative reputation event indicated that the biggest impact areas were revenue (41 percent) and loss of brand value (41 percent), followed by regulatory investigations (37 percent)

- Reputation risk is still a strategic business issue. 87 percent of the executives surveyed rate reputation risk as "more important" or "much more important," and 88 percent say they are explicitly focusing on reputation risk as a key business challenge. A reputation risk that is not properly managed can quickly escalate into a major strategic crisis
- Responsibility for reputation risk resides with the board and the senior executives. Companies participating in the survey indicated that responsibility for reputation risk resides at the highest levels of the organization, with the CEO (36 percent), Chief Risk Officer (21 percent), board of directors (14 percent), or CFO (11 percent)
- Customers are the most important stakeholders for managing reputation risk. Other key stakeholders include regulators, senior executives, employees, and investors
- Companies are least confident when it comes to risks that are beyond their direct control. Such risks include third-party ethics, competitive attacks, and hazards or other catastrophes. Companies are most confident about managing reputation risk drivers for which they have direct control, such as risks related to regulatory compliance, employee, and executive misconduct

These days, even issues that seem insignificant can become headline news and global reputations can be boosted or blasted with a few keystrokes. *"Leading organizations already treat reputation risk as a strategic issue—a trend that we expect will accelerate,"* says Mr. Ristuccia. *"The survey found, however, that many companies are underprepared to manage reputation risk. As reputation risk will likely be increasingly critical in the coming years, companies should continue to improve their capabilities in this area,"* he adds.



The top three drivers of reputation risk today are the same as the top drivers identified by companies that experienced a major reputation risk event in the past, according to the survey

* The findings in this report are based on a global survey of more than 300 respondents from the Americas (34 percent), Europe/Middle East/Africa (EMEA) (33 percent), and Asia Pacific (33 percent). Nearly all respondents were senior executives (126), board members (13), or specialized risk executives (169). The companies surveyed came from all five major industry sectors. For more information, visit www.deloitte.com/reputationrisksurvey.

Related Resources:

- Companies Underprepared to Manage Reputation Risk: Global Survey
- Using Social Media Governance to Protect Reputation
- Security Attacks: A Lead Driver of Reputation Risk
- Crisis Management: Preparing for the Next Big Event
- Creating Value from Risk: Owen Ryan, CEO, Deloitte Risk Advisory Services

Printed with permission by Deloitte & Touche LLP





21st century resilience

Getting it and keeping it

Michael Kearney

Partner
Advisory & Consulting
Deloitte US

Damian Walch

Director
Advisory & Consulting
Deloitte US

In the summer of 2015, nearly simultaneous “computer glitches” at three prominent enterprises caused many to wonder if there was a connection, and if perhaps some orchestrated attack was underway; even a government agency took an interest.

But a thorough search for the root causes revealed that each incident was entirely separate and distinct, originating in internally flawed systems. Even though there was no “grand design,” each failure cost the respective companies millions of dollars. They also served as startling examples of the vulnerability of major systems, and of just how common such disruptions have become.

In recent history, garden-variety human error and a malfunctioning relay were blamed for a partial power outage and a “rare electronics failure” at two national sporting events. Again, there was nothing sinister; just proof that when things can go wrong, they will go wrong.

Mobile devices not only help provide visual information, but they can also guide real-time decision-making

Faced with challenges from natural disasters and human infrastructure calamities, today's organizations need to be able to respond. Whether it is a mere technical glitch, human failure, or a full-scale catastrophe, there will still be an impact on day-to-day operations and, ultimately, on business reputations.

A risk-based world

The world in which we live is changing, and the threats we face in the 21st century seem to be growing both in volume and complexity. Each day, we grow more connected in terms of technology, economics, and infrastructure than we have ever been in the past. While natural disasters often grab headlines, human-caused events can also have widespread consequences. These can be innocent mistakes or deliberate attacks by hackers or terrorists. Yet because these disruptions are so deeply linked with the very nature of the businesses we conduct and how we pursue them, it is increasingly important to view risks as more intrinsic and ubiquitous than exceptional. They are no longer once-in-a-lifetime concerns.



In other words, risks are a part of the spectrum of operational factors that organizations should build around. To encompass those factors means focusing not just on "recovery" but also on agility and ever-greater resilience, so as to reduce the impact of events and speed up response. In short, organizations should consider the risk of their business decisions, integrating and strengthening their traditional crisis management capabilities under a new rubric that prepares them to be ready for anything.

Evolving perspectives

Traditional standards and fundamentals of Business Continuity Management (BCM) were largely defined between 1995 and the early 2000s. Unlike earlier times when production, distribution, and end customers were more loosely coupled (to cite an example from manufacturing), by the 1990s, the pace of business had greatly increased: shipments moved at a greater speed; organizations developed lean practices that improved efficiency but also eliminated cushions, such as large on-site inventories; increasing globalization in many



industries, particularly within financial services and the systems that sector employed, required 100 percent uptime in operations and the ability to facilitate huge transactions; and improving communications meant that customers could, and often did, change preferred providers whenever they believed it could be to their advantage.

Those developments not only tightened the links between a problem in one part of the value chain and impacts elsewhere, they also heightened the business consequences. At that point, organizations began to recognize their critical dependencies: sole-source suppliers, centralized data centers, and other key facilities that were “too important to fail,” because anything but the most rapid recovery could doom the rest of the business.

On that basis, companies built up disaster recovery capabilities and adopted practices that would help them ride out some well-defined “storms.” It was a necessary and correct response. But that came before social media, mobile technology, cloud computing,

and ubiquitous analytics; developments that further increased the speed of operations and, in many cases, led to new and poorly understood dependencies. In the face of this change, the business continuity management (BCM) discipline itself remained largely stagnant and non-innovative, propped up by habit and, frequently, by industry regulations and standards. What it provided was still important, but it wasn't enough.

Today, *instant* is the word, and 24/7/365 availability is the norm. Additionally, in the years since BCM became a defined activity, financial markets have become truly global and supply chains have continued to evolve, with less “slack” and more points in the chain that can cause critical problems when there is a failure.

The picture that emerges is one of multiplying risks that, in turn, further magnify other risks as they interact to produce complex events. A traditional recovery plan that sits in a notebook or on a hard drive and is reviewed each year or two (if at all) can scarcely keep pace with today's quickly developing and rapidly escalating challenges.

Mastering this world of risk and achieving resilience requires data—and lots of it. That is what enables organizations to make better decisions about necessary investments that help limit risks. Data also enables resilience by providing ample information to enable fully informed decision-making during incidents and “glitches.”

What kinds of data? Each organization will have different priorities and resources. But a balanced mix usually includes data on business processes, interdependencies, financial and operational impacts, certain support systems, and third parties.

These domains each track and use substantial quantities of data, which may not be readily accessible or in a form that is useful for discussing risk and resilience. Therefore, to guide both long-term planning and short-term resilience, it is important to identify specific potential sources of data and develop a plan for keeping it accessible and interpretable.

Traditional information from risk, business continuity, disaster recovery, and emergency response disciplines can also be assessed and, if possible, supplemented with geospatial information about facilities, business partners, and service providers. And as systems are refined and data is aggregated in a repository, mobile should be a component.

Mobile devices not only help provide visual information, but they can also guide real-time decision-making. Social media platforms can provide additional timely information about events and individuals to improve decision-making and reveal the outcomes of decisions already made.

In contrast to the sedate vision of BCM that has predominated for so long, today’s risk picture demands both speed and a response capability that is not an afterthought or an add-on. While it might once have been acceptable to frame risks around a laundry list of familiar natural or human-caused mishaps, such as fires and floods, that is no longer enough. Delivering

resilience in a 21st century context means having some kind of “decision engine” that enables an efficient and effective response to the risks and threats to which a company is exposed.

Getting there can take effort, but it should pay substantial dividends.

Moving toward resilience

Key risk indicators, the number of disaster plans created and catalogued, and frequency of updates were the foundation of BCM. Counting things may provide some metrics, but those plans rarely inform executives of their actual ability to respond to and recover from disruptions. A clearer indication is needed so that the data “counted” reflects the critical elements of the organization and its risk exposure. Data needs to be transformed into information that enables decision-making.

People are also part of the strategy. Risk and resilience belong to everyone in the organization. Tapping into the organization’s collective wisdom and orchestrating the results can make resilience part of the fabric of the business. Risk professionals need to engage at many levels in the organization to deliver this message.

For example, there are often many individuals who are cognizant of potential risks, but have no established means of sharing that information, usually because it is not something measured or rewarded. These risks could be challenges that are imminent or could emerge in the foreseeable future. Someone in the field may be aware of market sentiments that are on the cusp of gaining a troubling political dimension. Or an individual in purchasing may understand how a sourcing decision made elsewhere in the organization is leaving the organization vulnerable to a supply disruption. The point is that risk awareness, impact assessment, and resilient thinking should permeate the organization at least as much as awareness of profit and loss—perhaps even more so, since the consequences of risk can be so immense.

While risk needs to become everyone's job, awareness and knowledge of risk issues should flow upward in the organization, so they can be assessed on a strategic level and dealt with effectively, with the best possible resources.

The new resilience model also requires connecting people with data. A common problem is that some of the information needed to support resilience efforts is typically managed and accessed by only a small pool of people. Furthermore, there is typically plenty of data but because it isn't often organized as effectively as it needs to be, it is not immediately usable. Organizations typically have good information about their staff and facilities, their vendors and service providers, and their systems and applications. They may even have information about some specific kinds of risks and their potential impacts. However, that data has been created by different parts of the organization and resides in native files, file-sharing sites, or proprietary databases.

The data housed across the entity is not correlated to create meaningful information that can be used to assist the organization in understanding risk and composing resilience. It should also be noted that organizations have often acquired or developed point solutions—application inventories, risk databases, and business continuity systems abound—to address specific needs, but they typically do not integrate the data, and they lack an organizing principle tied to resilience. If an organization actually looked at each of those point solutions and made a concerted effort to integrate that data into usable information, it could provide executives with greater insight into their strategic and operational risk profile while helping point the way to resilience.

The bottom line is that companies are resilient when they are truly confident in their program, predictive about potential disruptions, and ready to be proactive in response.

Resilience confidence

The end result of resilience thinking should be resilience confidence: an objective, risk-based measurement, unique to each organization, which provides a clear sense of a company's ability to respond to disruptive business events, while also offering clear guidance on correcting underperforming areas. The starting point in this process should be visibility into risk. Various existing business continuity-disaster recovery, supply chain, and cyber information documentation and plans often contain useful information that can start the process. By themselves, they lack dynamism and offer comparatively limited response options. Together, they can be foundational elements for building resilience.

People are also part of the strategy. Risk and resilience belong to everyone in the organization

The new resilience model also requires connecting people with data

What does resilience confidence look like? It involves not only assessing risk but also determining what should be required to recover, replace, or rebuild critical business processes in the wake of business disruption and, in particular, the ability to meet recovery objectives. It is both a plan and a toolkit. But developing resilience confidence is a two-way street. For example, the loss of a single functional area might justify rapid recovery of that area—almost without regard to cost. Where multiple sites, functions, or facilities are affected, however, recovery may require tradeoffs, greater economies, or perhaps less rapid recovery goals. These possibilities and all reasonable recovery scenarios should be considered in advance. This not only prepares the organization to “weather the storm”; it also helps clarify dependencies among different sites and organizations, between and among technologies, and within the organization and its ecosystem of suppliers and customers.

Getting to resilience confidence can start with a simple checklist approach, but it should advance to include planning and discussion about potential scenarios, notification and activation processes, and descriptions of ultimate responses.

Boards of directors, with legal obligations regarding governance, should seek the kind of certainty that a resilience-confidence approach can provide. Put another way, there are no longer valid excuses for not anticipating specific kinds of disruptions or even combinations of disruptions. Also, boards will likely be held to the highest standards regarding how they have guided advanced preparations.

Executives, for their part, should be working to build resilience confidence, leveraging assets that are already in place whenever possible. This may yield rewards with modest efforts.

The great truth about resilience is that, as an attribute with day-to-day business value, it is not only helpful when disasters strike; it can strengthen an organization and help improve agility at every level. Resilience is an attribute to strive for and it may well be a requirement for the successful 21st century organization.

Conclusion

- Today, instant is the word, and 24/7/365 availability is the norm for achieving 21st century resilience
- Data is required to guide both long-term planning and short-term resilience. Identifying specific potential sources of data and developing a plan for keeping it accessible and interpretable is critical
- Making data accessible via mobile devices not only helps provide visual information, but also guides real-time decision-making
- Social media can provide additional timely information about events and individuals to improve decision-making and reveal the outcomes of decisions already made
- Getting to resilience confidence can start with a simple checklist approach, but it should advance to include planning and discussion about potential scenarios, notification and activation processes, and descriptions of ultimate responses
- Companies are resilient when they are truly confident in their program, predictive about potential disruptions, and ready to be proactive in response





Focus on Building crisis-ready boards

Peter Dent
Global Crisis Management Leader
Deloitte Touche Tohmatsu Limited

Dan Konigsburg
Managing Director
Corporate Governance & Public Policy
Deloitte Touche Tohmatsu Limited

It's different for boards

The view at the top is exhilarating. So is the weather. When crisis looms, board members are exposed in ways that may be unfamiliar – and drawn into an active role that's distinct from what management is going through.

Three out of four business leaders believe a crisis plan would benefit their organizations, yet barely half have a plan in place.¹ Even when there is an organization-wide crisis plan, however, that doesn't necessarily address the board's needs. Yes, the board supports the main plan with oversight, moral authority, and strategic vision. But the board needs a plan all its own for those moments that place it in the eye of the storm.

Threats to a company's value, reputation, or existence go beyond the operational level. Think about who outranks the board: shareholders. Regulators. Law enforcement authorities. If someone like that is involved, chances are the situation calls for a response at the highest level.

Then there are crises that directly involve the board or its members, such as litigation, leadership controversies, or even removing and replacing top executives. Making the board ready and resilient in the face of these threats starts with the composition of the board itself.

A different role in business means a different role in crisis

From the public's perspective, the board is seldom visible. Crisis, especially a leadership crisis, can thrust board members in front of media microphones. By that time, however, a lot should have happened behind the scenes.

A company and its board need to decide where operational issues end and "corporate crisis" begins. Of course, sometimes the difference between operational and existential crises isn't so clear. One can become the other quite quickly. The first category is usually the domain of the senior executives and the people who report to them – things like supply chain kinks or weather disruptions that complicate daily business. In contrast, a corporate crisis is one that involves reputation, share price, major litigation, regulatory sanction, or a company's existence. These may arise

from a number of sources: cyber threats, financial misdeeds, financial disruption, technological or industrial breakdowns, confrontations, or catastrophes that are outside anyone's control. And it may be up to the board to plan for the continuity of the enterprise in the case of an unforeseen disaster.

In preparing for, meeting, and rebounding from corporate crisis, the board isn't just in oversight mode anymore. Its members have a direct responsibility to anticipate threats and make quick, far-reaching decisions. That may include pre-populating a crisis subcommittee with people who excel in specific roles like legal, accounting, audit, public relations, or specific industry issues. It may include arranging for outside counsel or support, or deciding whom to include in sensitive external and internal communications, and whether to alert employees. The board's role at a time like this may even have to include replacing a CEO on short notice – or stepping in to act in that capacity for a time.

This is no place for on-the-job training

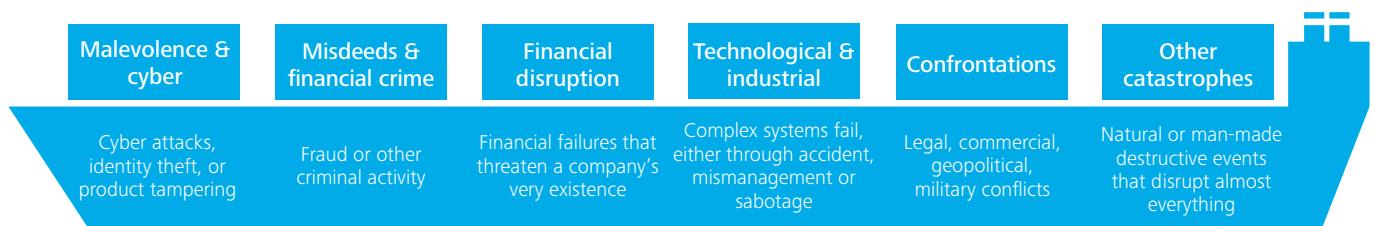
One valuable skill a board member may bring to a crisis is having been through one before. Whether an earlier trial ended well or poorly, whether the person in question earned the credit or bore the blame, firsthand experience ingrains more than knowledge in a person – it also instills confidence and poise under pressure. It's true that crisis experience may not be at the top of the checklist when boards recruit new members. A board member's crisis service on one board may seem to be a distraction from service on another. And the prospect of dealing with a bad situation is probably not the reason people seek or accept board appointments. But in the final balance, experience is still the best training and a valuable quality to build into a board's mindset. It is hard to weather a storm with a group of people who came together with smooth sailing in mind.

Nor is crisis the right time to discover disharmony. When the job suddenly expands far beyond quarterly reports and shareholder meetings, any cracks are going to become very visible and very costly. Only a dedicated crisis plan can set the board on a path toward crisis resilience, and only formal simulations can determine how well the plan and the people will really function when they have to.

¹ "Crisis Survey 2013" (Burson-Marsteller, 2013)

A world of crisis triggers

Crises can be malicious, accidental, or completely random. Most organizations are susceptible to threats from more than one of these potential triggers:



Know the lay of the land

The relationship between organizational crisis planning and board crisis planning takes its cues from the relationship between the organization and the board. Historically, there have been important regional differences in this alignment, though they are declining. In the United States, the CEO is typically invested with significant strategic latitude – and may also be the board chair. In Europe and Asia, the senior executives may take strategic cues from a more prescriptive board. Each organization should assess these lines of authority and make sure the plan for action in a crisis corresponds to them. Some CEOs will look to the board during major threat events. Others may risk feeling micromanaged. To avoid misunderstandings when no one has time for them, it's important to have regular, honest discussions about who expects what from whom.

No matter what the board's intended role in crisis management is, it needs timely, accurate information. If some board members are accustomed to receiving the information management provides them with, this may require the development of new antennae, and a renewed willingness to ask tough questions. To maintain a 360-degree view of the threats it faces, a board may look to third-party or public data. It may also consider whether it should secure access to the real-time operational data that's usually the province of people lower down on the org chart. Deciding what information to watch is a matter of strategy; making it happen can become a question of technology and processes.

How to start

Know what you're getting into. Membership on a board of directors usually starts with an appeal to your experience, connections, or even vanity. The setting is august, the time commitment limited. But when crisis strikes, board members become full-time leaders – and stay that way until the threat subsides. People who join a board may not expect daily conference calls to be part of the bargain, but they may be the most important engagements a person has during his or her tenure.

Embrace the unglamorous part. Facing down reporters, regulators, and shareholders in a moment of high drama is only part of the crisis task. Before any of that happens, crisis management includes meetings, reading, briefings, and day-long simulation exercises. Before you can master the three-ring circus, you need to embrace the three-ring binder. This is work. But it pays off.

Identity is planning. Who on your board is expert in risk? Who is the steady PR hand? Who knows how to monitor social media and safeguard reputational risk? And who has been through something like this before? If you build crisis capabilities into the very makeup of a board, define the role of the board, and agree upon the operating protocols in a crisis, it will be easier to staff the necessary subcommittees, determine the need for outside advisers, and plan roles and responsibilities. Whether the solution is a phone tree or a written protocol, any solution is better than finding that no one knows who is in charge.

Special boards, special considerations

No organization, nor every board, has the same responsibilities – and in some cases, the right approach to crisis planning changes to match the circumstances.

Family-owned organizations

When the board reports to a family owner, crisis can also come from unusual directions – and it can include things the directors aren't accustomed to discussing with the family. A lack of succession planning is one vector for trouble. Crisis can also arise from ineffective family decision making or from emotional disputes.

Boards and families both tend to avoid these tough conversations until it's too late. It can help defuse problems if they get ahead of topics such as estate affairs, future leadership positions, family members' future plans, preparing the next generation, conflict mediation, and how closely the company's market position is tied to the personalities of the founders.

It can be hard to do two things at once – to recognize the divide between business and family matters while paying careful attention to the places where they overlap. One mechanism that can help address this is the creation of a family council that sits alongside the board of directors. On a higher level, though, the best tonic is open and honest communication.

State-owned organizations

A crisis may place considerable pressure on corporate governance of a state-owned entity (SOE), but it may also present a unique opportunity for independent directors to prove their value to the company. An SOE has particular obligations to a society and an economy – and when the contribution it makes comes under threat, experienced board members can play an important advisory role in the space between the organization and the government to which it reports.

If public-sector officials reach out to executives directly in a crisis, board members may feel their roles becoming diluted. It's also possible that government representatives on the board will feel unwilling to expose themselves to criticism by providing tough guidance when it's needed most. But if the board prepares for a central crisis role and asserts itself when the moment arises, members can use their experience to make calls that decision-makers above and below them aren't able to make. And when the crowded hour has passed, they can leave a legacy of stronger governance and better crisis resilience.

Boards in action

Serious violations, serious remediation

A global technology company faced a criminal investigation following charges of bribery and corruption. As police raided homes and offices, prosecutors made arrests, and the share price tumbled, the board's Audit Committee determined to get ahead of events and restore trust by carrying out a comprehensive investigation of its own. It established an independent Compliance Committee and retained outside legal and forensic help. Advanced analytics, personal interviews, transaction analysis, and business intelligence helped the company understand where violations had occurred and where controls had broken down – and indeed, the investigation did uncover improper acts. Though the potential fines were large, the World Bank and regulators in multiple countries credited the company for its transparent investigation and diligent remediation. Today the company is viewed as a leading practitioner of anti-corruption compliance.

No one knows when a turn of events will demand the best your organization can deliver. No matter what form it takes—whether it's front-page news or a quiet struggle only you know about—crisis is a moment of truth that tests your readiness, resilience, and character.



Focus on The board's-eye view of cyber crisis management

Peter Dent

Global Crisis Management Leader
Deloitte Touche Tohmatsu Limited

Nick Galletto

Global Cyber Crisis Management Leader
Deloitte Touche Tohmatsu Limited



Forget about being an observer

The board's chief role in the organization may be oversight, but board members are increasingly being pulled from their elevated vantage point into the thick of cybersecurity issues. The possibility of being held personally liable in the event of a breach is one motivator to roll up their sleeves. Another is the ripple effect a cyber crisis can impose on the organization. A website going down is one thing; the company going down is another.

The fallout from many breaches often includes costly drawn-out litigation, distracting regulatory actions, trickle-down operational disruption, impaired strategy execution, and increased insurance liability, all of which diminish corporate value.

Beyond business: This is personal

The reputational stakes for board members are high. Shareholders have responded to some cyber breaches by calling for removal of some board members or filing derivative lawsuits against the directors and officers, alleging, for example, misconduct and breach of fiduciary duty, both before and after the cyber breach. Board members of companies involved in a cyber incident may see impacts to their reputation and effectiveness as scrutiny and attention continue to mount over cyber incidents.

Class action lawsuits have become more common on the heels of a cyber breach, often with more than one suit filed. Regardless of the outcome of a suit, external and internal legal fees nonetheless mount throughout the class proceedings, making class actions lawsuits costly.

Threats of operational impairment

Beyond the personal threat, board members must also contend with the ways a breach can trigger widespread disruption far beyond the initial point of attack, and in turn, greatly magnify losses.

Consider today's tightly integrated, demand-driven supply chains. The same cyber functionality that enables great efficiency along the chain — from raw materials procurement to production to inventory and distribution — also introduces vulnerability at every link. A hack that brings down a vital piece of equipment, sometimes for only a few hours, can start a chain reaction. Disruptions in procurement impede production, which can deplete inventories and result in the inability to fulfill orders. As each link in the chain is impaired, financial losses mount.

Compromised growth

M&A and joint ventures can be particularly vulnerable to the fallout from cyber breaches. Cyber espionage in these deals has become all too common, with cyberattacks launched in hopes of gaining financial

or operational intel to use as leverage in negotiations. Cyber breaches can also be used as a means to devalue a company on the grounds of weak defenses and failure to properly address risks.

Relationship risks

The tight integration many companies have with their suppliers and vendors means their company is susceptible to third-party risks. A third-party breach could quickly jump inside the organization's four walls to compromise operations and create a liability issue. Viewed from a third-party's perspective, a breach or inadequate defenses in an organization could result in vital suppliers declining to do business with them, fearing the risk of disruption to their organization.

Beyond litigation — insurance implications

Cyber breaches pose another danger that many boards fail to consider: the effect on insurance. Some companies and board members have taken comfort in having insurance to cover liabilities due to breaches. Data breach or cyber insurance policies are becoming an important part of a company's preparedness plans. In 2013, only 10 percent of survey respondents said their company purchased a policy. In 2014, the percentage more than doubled to 26 percent.¹ Insurance providers, however, have become increasingly focused on examining the root cause of such breaches. If companies are found to be negligent in their defenses or in following leading practices, their insurance payouts may be reduced or even declined.

A three-pronged approach

The board plays an important role in helping the organization determine how to respond to the new cyber threat landscape. Boards should challenge management to assess the organization's cyber posture and critically review its cyber crisis management capabilities. Crisis management starts with identifying and preparing for the risks of a cyber incident that may turn into a crisis and building a broad portfolio of capabilities, such as event monitoring, crisis simulation and planning, real-time response, and crisis communications. While the number of companies that have data breach response plans in place is growing, more than a quarter (27 percent) of companies still do not have a plan in place.²

Preparedness is more than checking a box or passing a test: it requires understanding where the organization's prized assets are and how criminals may try to compromise them. Cyber risk management begins with securing risk-sensitive assets. If the assets at the heart of your organization's mission are not properly protected, they are open to risks that can turn into major business-threatening crises. At this point, cyber risk management turns into cyber crisis management. In order to be prepared for a crisis, organizations must be **vigilant** in monitoring for threats against them and **resilient** in recovering from a breach as quickly as possible should an event occur.

A world of crisis triggers

Crises can be malicious, accidental, or completely random. Most organizations are susceptible to threats from more than one of these potential triggers:



Malevolence & cyber

Cyberattacks, identity theft, or product tampering



Misdeeds & financial crime

Fraud or other criminal activity



Financial disruption

Financial failures that threaten a company's existence



Technological & industrial

Complex systems failure, either through accident, mismanagement, or sabotage



Confrontations

Legal, commercial, geopolitical, military conflicts



Other catastrophes

Natural or manmade destructive events that broadly disrupt

¹ *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness*, Ponemon Institute, September 2014

² *Ibid*

To be **vigilant** means that an organization is in a better position to predict and prevent security incidents; it has a custom approach to cyber intelligence that identifies threats specific to the organization's environment and continuously evolves. Cyber threat intelligence and cybersecurity awareness should be emphasized at all levels of the organization. In fact, many cyber breaches enter through phishing emails that are opened by staff and inadvertently launch malicious code into the technology environment.

Resilience is key in the event of a breach; organizations should respond rapidly to contain the incident and prevent its spread. While resilience requires investment in traditional technology-based redundancy and disaster recovery capabilities, the bigger picture also includes a broad set of cyber crisis management capabilities. This is where plans are put to the test and immediate, on-the-ground incident response is used to analyze the breach, stop the damage, and mitigate any after-effects.

Boards must challenge management to confirm the organization is proactive, clearly understands the effectiveness of its cybersecurity program, and is focused on the right things:

1. Know your crown jewels – not just what you want to protect, but what you need to protect
2. Know your friends – contractors, vendors, and suppliers can be security allies or liabilities
3. Make awareness a priority – within every internal department and among external parties
4. Fortify and monitor – diligently gather intelligence; develop situational awareness; build, maintain, and proactively monitor defenses
5. Prepare for the inevitable – test your incident management process

How to start

Commit to evolving

The board should hold management accountable for implementing a cyber crisis management plan and for building cyber resilience capabilities that address the unique risks to the organization. Furthermore, the plan should be regularly measured for effectiveness and should continually evolve over time. Cyberattacks are constantly evolving, and the board should confirm the organization can evolve as well.

Test capabilities and learn from the results

In order to be effective during a cyberattack, the board should ensure the organization's cyber incident response is tested and shown to be effective in a simulated attack. Results of simulations should be used to correct weaknesses in security, vigilance, and resilience.

Don't try to go it alone

The board should ensure that its organization is prepared with subject matter experts who can be on the ground as soon as security is compromised. An external team can organize the chaos and keep your management team focused on running the business. The team should include not only cyber specialists, but also public relations, legal, and other professionals to enable you to act quickly to address the aftershock of the breach. An emerging boardroom practice is for directors to invite cybersecurity subject matter experts to provide advice and perspective to the board.

Cyber crisis management in action

A top five priority

In an effort spearheaded by the board's concern about the potential for a security crisis, a global energy company adopted cybersecurity as one of its top five organizational priorities. The board took it upon themselves to seek the counsel of a leading security adviser who outlined the specific threats to the organization. The board then queried executive leadership about the company's cyber strategy, which led to the development of a comprehensive and coordinated organization-wide approach. Cybersecurity requirements in each business unit are being aligned throughout the enterprise in accordance with leading industry standards and practices — but more importantly, in proportion to the actual threats facing them.

No one knows when a turn of events will demand the best your organization can deliver. No matter what form it takes—whether it's front-page news or a quiet struggle only you know about—crisis is a moment of truth that tests your readiness, resilience, and character.





The benefits and limits of cyber value-at-risk

Jacques Buith
Managing Partner
Clients & Industries Leader
for Global Risk Advisory
Deloitte Netherlands

Dana Spataru
Senior Manager
Risk Services
Deloitte Netherlands

The World Economic Forum's Partnering for Cyber Resilience initiative developed a preliminary framework for a statistical model which CIOs and other executives can use to begin quantifying the financial impact of cyber threats.

Many CIOs across industries struggle to answer questions about cyber risk posed by their executive teams and boards of directors: How likely are we to experience a damaging attack? How effective are our existing risk mitigation measures? If we spend US\$20 million more on cyber risk mitigation, how much would that reduce our risk?

In the interest of helping organizations answer these and other questions, members of the World Economic Forum's Partnering for Cyber Resilience initiative recently proposed a working model for measuring and quantifying the impact of and exposure to cyber threats. Known as cyber value-at-risk, the model provides a starting point for quantifying risk and attempts to inject more discipline into that process, although it requires further refinement and field-testing.

With a goal of allowing corporate leaders to quantify more of the cyber risks their organizations face at a more granular level, cyber value-at-risk ultimately seeks to help them make more informed, confident decisions about their organization's risk tolerances and thresholds, cyber security investments, and other risk mitigation and transfer strategies.

Despite the current challenges in applying the model, companies that have been exposed to cyber value-at-risk express enthusiasm for it. One organization working with the World Economic Forum's cyber resilience initiative obtained a more structured view of its risk profile by using the model, and now the organization is making more fact-based security investments and policy decisions as a result.

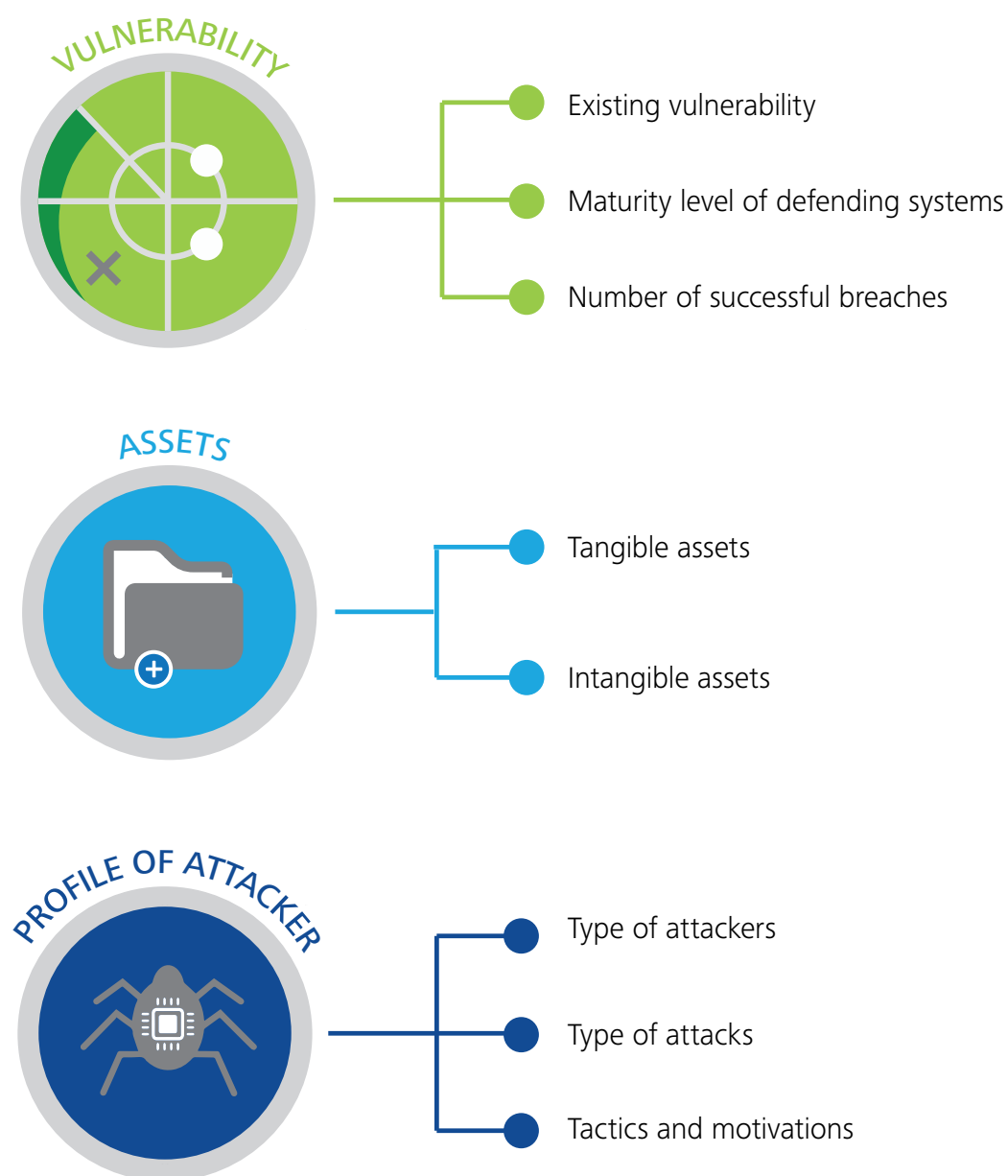
The roots and components of cyber value-at-risk

The concept of cyber value-at-risk is based on the notion of Value-at-Risk (VaR), a statistical technique widely used in the financial services industry to express a bank's level of financial risk (or the financial risk associated with a specific investment portfolio) over a specific period of time. Similarly, cyber value-at-risk seeks to use probabilities to estimate likely losses from cyber attacks during a given time frame.

Cyber value-at-risk considers three primary drivers, or components, of cyber risk for an organization: its vulnerability, its assets, and the profile of its potential attackers. Analyzing dependencies among the three components is critical to estimating risk exposure using cyber value-at-risk. For example, the number of attacks a company is likely to experience largely depends on the value of its assets to potential attackers and trends in the attacker community. Therefore, the company's assets and the attacker profile determine the extent to which the company may be a cyber-attack target.

Cyber value-at-risk considers three primary drivers, or components, of cyber risk for an organization: its vulnerability, its assets, and the profile of its potential attackers

Figure 1: Cyber value-at-risk components



Source: World Economic Forum, "Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats"

One of the biggest challenges associated with obtaining accurate results from cyber value-at-risk is the ability to estimate the probability of a successful attack

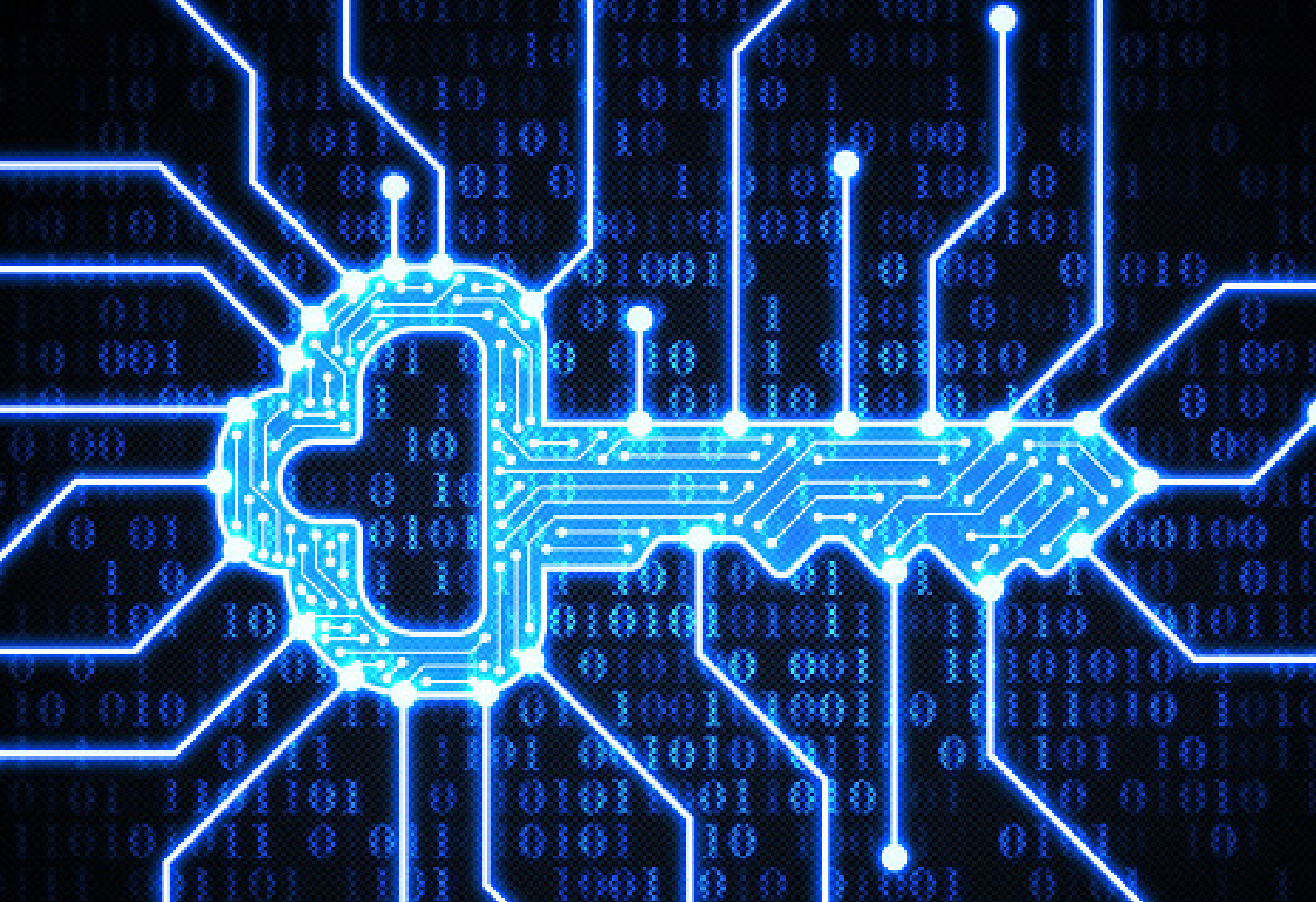
Vulnerabilities take into consideration, for example, the number of unpatched systems inside an organization, the number of previous compromises it has experienced, and the maturity level of its defending systems as defined by the number of security updates applied, the number of defensive software components installed on the network, and the network typology and infrastructure.

Assets vary by organization, but on the tangible side, they typically include funds and financial instruments, infrastructure, production facilities, and financial losses incurred through temporary business disruption, complete business interruption, and regulatory fines. On the intangible side, assets frequently encompass intellectual property (IP), customer or employee data, and a company's reputation.

Attacker profile looks at the type of attackers, whether they are amateurs, state-sponsored, or part of organized crime rings; their motivations (e.g., financial gain, theft of trade secrets, destruction, reputation damage); and the sophistication of the attacks they tend to perpetrate.

The limitations of cyber value-at-risk

One of the biggest challenges associated with obtaining accurate results from cyber value-at-risk is the ability to estimate the probability of a successful attack. Doing so requires a large set of real-world historical data regarding the frequency and severity of risk events that is not yet widely available, for the reasons that follow. Obtaining reliable cyber risk data is hindered in part by delays between the time cyber events occur and when organizations detect (and report) them. Given that current regulations in the United States require reporting on only a subset of cyber attacks, the availability of data to understand, for example, attacker behavior is likely to remain limited until a broader culture of cross-industry and public/private sector information sharing takes shape. (Some of these regulations include the Health Insurance Portability and Accountability Act's breach notification rule and various states' security breach notification laws.)



Furthermore, the range of possible vulnerabilities an attacker may exploit may not be perfectly quantifiable: software vulnerabilities sometimes remain unidentified for years; dependencies on third-party infrastructure may limit visibility into the status of various assets; and the ability to anticipate future or evolving attacker motivations is an imperfect science. The degree of complexity and rate of change in many environments will continue to require an emphasis on establishing vigilance to detect the unexpected and resilience programs to support business recovery when a successful attack does occur.

The lack of standard maturity frameworks also limits cyber value-at-risk's current effectiveness. The number of incidents an organization is likely to experience depends in part on its relative cyber maturity, but without a standard maturity measure applicable across industries, quantifying threat "attractiveness" remains more subjective than objective.

Finally, cyber value-at-risk supports only a limited number of risk scenarios at this time. The probability and impact of outlier incidents, like an attacker stealing a waste management company's credentials to a client's systems in order to compromise the client's network, remain difficult to determine using cyber value-at-risk.

The future of cyber value-at-risk

It took the financial services industry 30 years to refine value-at-risk to the point where it is useful and trustworthy. Honing cyber value-at-risk will also take time, but those who invested in the model are working diligently to craft a usable version.

With a conceptual framework for cyber value-at-risk established, a next step is applying real-world data to the model. Our hope is that exposing the potential benefits of cyber value-at-risk will prompt industry participants to share more of the data needed to make the model work effectively. In the meantime, CIOs can use the notion of risk-based quantification to position themselves to use the cyber value-at-risk model and justify budget requests to the executive team and board.



A holistic approach to regulatory watch

Simon Ramos

Partner
EMEA Investment Management
Regulatory Leader
Deloitte Luxembourg

Marc Noirhomme

Director
Advisory & Consulting
Deloitte Luxembourg

Laurent Dao

Consultant
Advisory & Consulting
Deloitte Luxembourg



A recent Deloitte survey revealed that most financial institutions have now realized the importance of the regulatory watch function for remaining ahead of regulatory challenges. With a holistic approach that combines regulatory watch, compliance, legal, and business functions, it does not have to be more complicated than it already is.

Why do we focus now on regulatory watch?

Following the global financial crisis that started to emerge in 2007, the political, regulatory, and supervisory responses have had major implications for the financial services industry.

1. Regulatory landscape

The unprecedented regulatory weight has forced financial institutions to develop and broaden the full range of skills and tools necessary to address technical matters and to keep up with an evermore complex regulatory landscape.

2. Costs of regulatory transgressions

Penalties for non-compliance have reached unprecedented levels. According to the *Financial Times*¹, Wall Street banks and their foreign counterparts have paid out US\$100 billion in U.S. legal settlements since the financial turmoil. If one believes that regulatory compliance has become too expensive, non-compliance would certainly be far more costly. While some institutions—usually smaller institutions with limited resources—have been tempted to adopt a risk-based approach toward regulatory compliance, this is nowadays a very risky decision.

¹ *Financial Times* (25/03/2014): “Banks pay out \$100bn in US fines” (R. McGregor and A. Stanley)

3. Tighter scrutiny from supervisory bodies

Supervisory authorities have not only become increasingly demanding in terms of reporting and liquidity and capital requirements, but they also pay more attention to the strategies and business models chosen by their supervised entities. Board members and senior management are also being increasingly held accountable for the consequences of their decisions or lack of action. Financial institutions that are most likely to thrive in this environment will be those that understand what an adequate or sustainable strategy and business model look like from a supervisory perspective. To satisfy the increasingly demanding supervisors, they would also need to have the vision to extract the maximum possible benefits from the investments they make.

4. Multiple sources of regulatory information

The demand for greater scrutiny has been accompanied by an emergence of new supervisory entities (e.g., the new European Supervisory Authorities) as well as an increase in staff members.

With each supervisory entity publishing its own publications (e.g., guidelines and consultation papers), financial institutions have become overwhelmed with regulatory updates. In addition, law firms, consulting firms, global custodians, and industry associations also publish newsletters and alerts.

5. Generic vs. specific information

Despite the high volume of publications available, the majority tend to contain rather generic information that is not specific to organizations. The challenge for financial institutions consists in figuring out which publications are really important and which will enable them to anticipate the specific business impacts.

In a nutshell, what should an efficient regulatory watch consist of?

1. Set up of the function

First of all, businesses need to define the organization of the regulatory watch function. This includes determining the ownership of the function (e.g., compliance, legal, strategy, etc.) as well as the roles and responsibilities of all stakeholders involved, namely the watchers and business experts.

2. Screening and monitoring of changes

In the second step, sources that will provide the relevant information in line with the activities and services of the institution should be identified. If the institution has an international footprint, it should also ensure that the scope of the watch covers both local and cross-border needs. This phase is key to ensure that the relevance, scope, and volume of information are well-suited to the organization.

Watchers can then start screening the pre-selected sources and monitor existing topics, capture new ones, and prioritize them for further action. In parallel to the screening, the institution should set up means of storage and communication to transfer information to business stakeholders.

3. Pre-assessment of impacts

To enhance the use of the regulatory watch input, a pre-analysis should be performed and its results shared with business stakeholders at the right moment. Keeping business units informed on a regular basis about upcoming regulatory changes will foster anticipation and facilitate project implementation. Bespoke information about regulatory updates should also be shared with the different compliance stakeholders such as the board and local entities.



4. Detailed business impacts

Based on the pre-analysis, the organization may decide to conduct in-depth impact analysis. To coordinate horizontal impacts, it is recommended to involve every stakeholder from the beginning—not only compliance but also the executives, legal, IT, risk, and business units. This is the essence of the holistic approach to regulatory compliance.

5. Gap analysis

Following the business impacts, a gap assessment clearly identifies what needs to be changed in the organization. It is a prerequisite for the implementation project that actions mitigating these gaps are planned and the required resources are identified (i.e., volume and type).

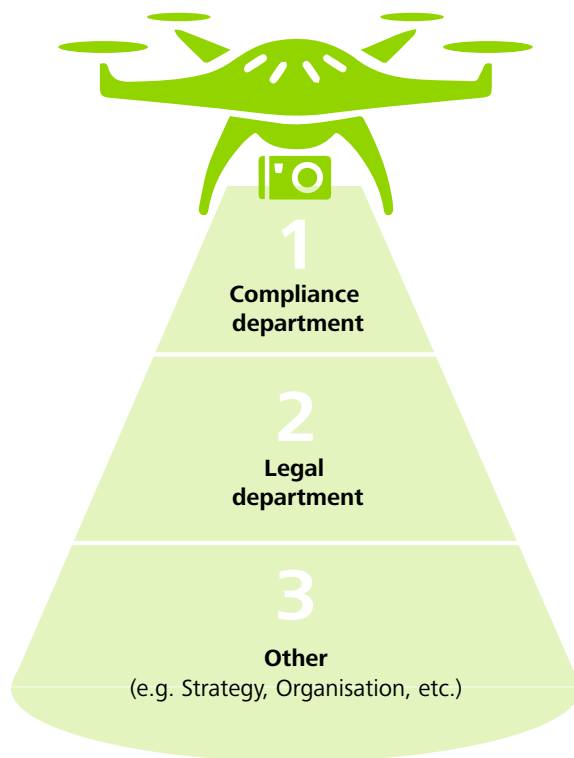
6. Implementation

Finally, once the appropriate resources of those involved in the Business as Usual (BAU) are mobilized, the Project Management Office (PMO) can coordinate the implementation and post-mortem implications.

First of all, businesses need to define the organization of the regulatory watch function. This includes determining the ownership of the function (e.g., compliance, legal, strategy, etc.) as well as the roles and responsibilities of all stakeholders involved, namely the watchers and business experts

Deloitte survey

In light of the regulatory burden that has fallen upon financial institutions, Deloitte decided to conduct a survey on the organization of the regulatory watch function. The survey aimed primarily to better understand how financial institutions collect, examine, and manage information on current regulatory developments, and how it is embedded in their organizations.



1. General overview of the survey respondents

The survey covers financial institutions, particularly those active in the pan-European market. The majority of the respondents are institutions whose primary business is in private banking, investment banking, or universal banking. The remaining participants are actors operating in the investment fund industry (e.g., custodians, management companies, and fund administrators).

With regard to their geographical footprint, half of the survey respondents are local Luxembourg institutions with limited foreign implementations. However, a quarter of respondents are global institutions with six or more branches or subsidiaries abroad.

2. Ownership of the function

Results of the survey show that the regulatory watch function is generally a duty of the Compliance Department, and in some cases part of the Legal Department. Nonetheless, a minority of respondents are conducting this function within other specific departments such as organization or strategy.

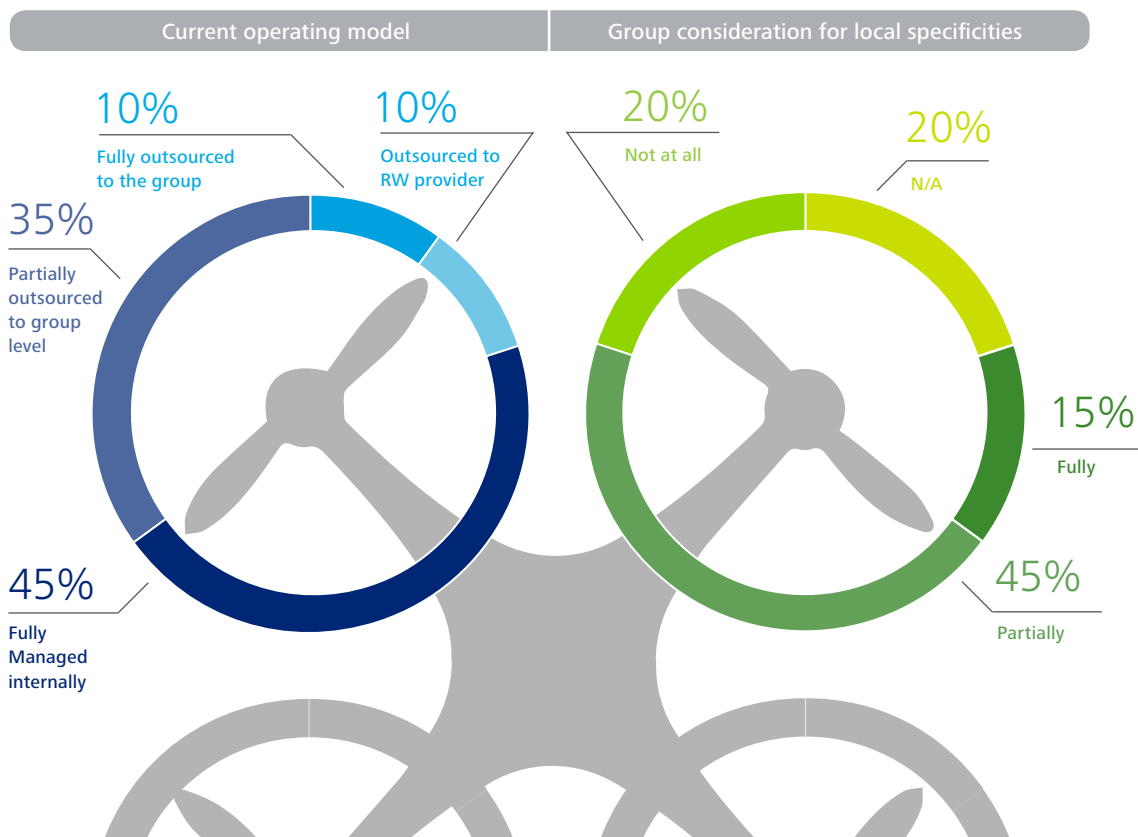
Moreover, the way that organizations view the function largely varies across institutions. 40 percent of the survey respondents view regulatory watch and monitoring as a silo-driven activity (e.g., a sub-part of the Compliance or Legal Department), while 35 percent of the survey respondents consider it a combined function embedded in the compliance and business function. Only a minority of institutions adopt a holistic approach where the regulatory watch and monitoring blends legal, compliance, strategy, business, and operational aspects into one.



3. Set up of the regulatory watch function

For most survey respondents, the regulatory source screening function is generally performed internally, either fully or partially at the local level. 45 percent of respondents have indicated that they delegate the function to the group (35 percent partially, 10 percent fully), and only a minority have outsourced the function to an external provider such as a regulatory watch and monitoring provider.

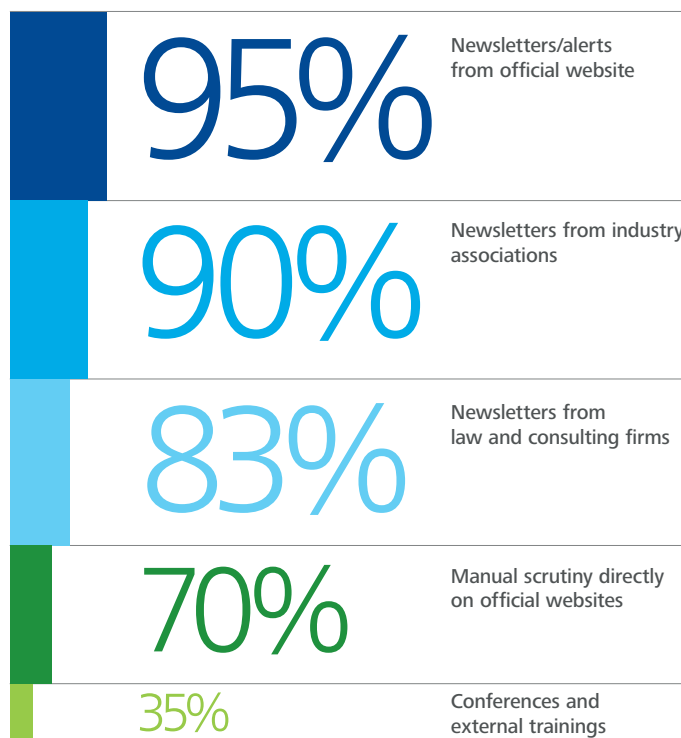
Out of the respondents who have outsourced partially or fully the source screening function to the group level, 45 percent of them have indicated that their local specificities are only taken partially into account by the group. One in five even state that the group does not take into account their local specificities at all. This reflects how difficult it is for any group to follow the regulatory status in each country where it operates.



4. Identification of the sources for screening

The results of the survey highlight the fact that most institutions only follow a limited number of sources, generally less than 10.

Group entities or companies with international practices are nonetheless required to follow additional sources to cover the entire scope of their activities. The vast majority of survey respondents follow a combination of sources and information channels. Newsletters and alerts prepared by the competent authorities or industry associations are the most common information institutions to which they subscribe. Information provided by law and consulting firms is also used by many. The survey suggests that respondents generally prefer to follow information already selected and pre-analyzed by experts rather than raw data from official websites.



5. Number of resources required

The conduct of the regulatory watch function may require a significant number of resources as many respondents employ one to two full time employee(s) (FTE) solely as regulatory watchers. However, this figure must be analyzed with the size of the institution in perspective. For examples, larger institutions with 200+ employees—representing 46 percent of the survey respondents—can more easily afford to allocate one to two FTE as watchers, compared to smaller institutions with less than 50 staff members. In fact, the results of the survey reveal that duties of the regulatory watch are also commonly delegated to part-time employees.

Figures among respondents vary with the number of sources being watched, but the majority of the survey respondents indicate that on average one FTE could manage up to 10 different sources.

Firms that may lack the capacity to monitor more than 10 regulatory sources may be missing out on critical information. Let's not forget that local regulatory specificities can be make-or-break.

6. Automation and frequency

The results of the survey highlight the fact that most institutions perform the regulatory screening manually, and some respondents have outsourced this process to providers that have automated the regulatory screening with the support of a web-based tool.

With regard to the frequency of the watch function, the majority of the respondents are performing their regulatory watch on a weekly basis. This is in contrast to a quarter of the respondents who are performing their screening on a monthly basis and only a minority who perform it daily.

7. Reporting of regulatory updates

Only 20 percent of the survey respondents use a central repository as a tool for storing and sharing regulatory updates. In that context, most institutions use emails or arrange meetings to discuss regulatory changes. A combination of traditional communication channels are used by almost half of the survey respondents.

8. External service providers

In a resource-constrained environment, where it is difficult to deprioritize any compliance-related task, freeing up time by using a regulatory watch service provider can be invaluable.

In that sense, 75 percent of the survey respondents consider regulatory watch services valuable, while the remaining respondents would consider it depending on the scope and bespoke service. Moreover, the majority of the respondents have also expressed their interest in a tax watch and monitoring service, often to complement the regulatory watch function.

In fact, the increase in proactivity toward addressing negative regulatory changes is seen by many as the most important aspect of a regulatory watch and monitoring service.

Conclusion

A combined approach of compliance, regulatory watch, and business functions is essential to fully grasp the implications of upcoming regulations, mitigate risks, and prevent what might otherwise be huge compliance challenges.

When looking at the market, the survey has highlighted that only a minority of businesses currently employ a holistic approach to regulatory watch. However, the survey respondents have recognized its importance and are now considering a similar approach. In that regard, regulatory services providers can certainly provide valuable support to institutions overwhelmed with regulatory changes.

Only time will tell which institutions have successfully managed that transition and have turned regulations into competitive advantages.

To the point

- We have witnessed an unprecedented regulatory weight on financial institutions that have tried their best to cope with regulatory updates
- A flexible, efficient, holistic, and proactive approach to regulation can make changes more manageable. But one should keep in mind that one size does not fit all
- Deloitte's survey reveals that most firms perform the source screening manually and do not use any tool or support from external parties
- The use of a global repository to share and store regulatory updates and analysis offers some great advantages
- Regulatory watch service providers can be invaluable for freeing up time and resources, allowing organisations to refocus on core compliance issues



Exponential change

Hot topics for internal audit in financial services for 2016

Paul Day

Partner
Financial Services Internal Audit
Deloitte UK

Kanta McNeill

Senior Manager
Banking Internal Audit
Deloitte UK

Seb Chung




Manager
Banking Internal Audit
Deloitte UK



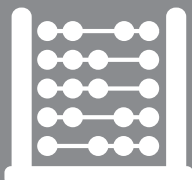
2016 will be another year of exponential change and internal audit departments in financial services will need to keep abreast of technology developments and adjust to new regulatory requirements while managing emerging risks and meeting ever-expanding stakeholder expectations.

Introduction

Financial services organizations continue to operate in an environment of exponential change due to continued advances in technology, adoption of new regulations, and competition from new entrants to the sector.

Internal audit plans for 2016 should be developed keeping in mind the exponential changes that will have an impact on the financial services industry. Internal audit departments have to adjust and adapt to the regulatory requirements, emerging risks, and competition affecting the industry. This change presents a unique opportunity for internal audit departments to lead as a catalyst for change in their organizations for the longer term.

			
Business leadership	Risk management	Regulatory matters	Capital and liquidity
<ul style="list-style-type: none"> • Corporate & risk culture • Communication • Individual accountability • Annual audit opinions 	<ul style="list-style-type: none"> • Risk appetite framework • Insurance coverage • Operational risk • Model risk 	<ul style="list-style-type: none"> • New regulators • Retail conduct • Financial crime • Client assets 	<ul style="list-style-type: none"> • Solvency II • Data quality • CRD IV

		
Trading	IT	Accounting and tax
<ul style="list-style-type: none"> • Product & valuation controls • Fair and Effective Markets Review (FEMR) • Unauthorised trading • High frequency and automated trading 	<ul style="list-style-type: none"> • Cyber crime • IT Disaster recovery and resilience • Digital forces • Continuous risk assessment 	<ul style="list-style-type: none"> • Tax risk management • COSO 2013 framework



Business leadership

Corporate & Risk culture

Many internal audit professionals agree that risk culture assessment is not a fad; risk culture measurement, monitoring, and management have been “hot topics” on regulatory agendas since the financial crisis in 2008. Financial services organizations have continued to develop their risk culture assessment programs as most organizations now recognize that risk management processes, systems, and internal controls are only as good as the behavior of the people operating or overseeing them. The debate within internal audit has moved from discussing whether risk and control culture should be included in the risk-based audit plan to what granularity of risk culture should be covered in its audit plan.

As a result, there has been a shift in the work performed by internal audit departments from generic risk and control culture audits to specific audits on a more granular sub-risk culture for areas like conduct risk, operational risk, and market risk. Risk culture assessment is becoming an established measure for assessing the quality and embedding of an organization’s strategic plan, risk appetite, governance structure, risk management, and remuneration framework. It is becoming increasingly common for internal audit to include aspects of assessing organizations’ risk and control culture in their annual planning process.

Communication

Communication is the process of transmitting messages or information by an organization internally (with staff) or externally (customers, regulators, or other stakeholders). Organizations’ communications are fundamental to helping customers make informed decisions. Regulators are developing expectations that organizations embed an organization-wide culture where the importance of effective communication with customers is recognized and prioritized.

Customers are increasingly using social media to engage with an organization and if managed appropriately this can be a very effective way for organizations to engage with their customers. However, when things go wrong, social media is an additional and more real-time channel through which an organization can incur reputational damage given 24/7 coverage by news channels on “viral” events (including corporate events). It is therefore critical that organizations effectively manage their

communication channels and that they consistently convey the proper tone in their communications in a timely manner, regardless of the medium used.

Individual accountability

Clear, defined individual accountability helps to drive up standards, and make organizations easier to run and to supervise. And if things go wrong, it will allow senior managers to be held to account for misconduct that falls within their area of responsibility. It will also hold individuals working at all levels within relevant organizations to appropriate standards of conduct.

In the UK, the regulators have given enhanced attention to this area by introducing a range of policy changes that aim to increase individual accountability within the banking sector. The regimes for senior managers, conduct, branches, remuneration, and whistleblowing will be applicable to in-scope financial organizations. Many organizations are currently reviewing and re-designing roles, governance arrangements, policies, and processes in order to meet the regulatory requirements.

Annual audit opinion

Providing an opinion on the design and operating effectiveness of the organization’s internal controls continues to be challenging for internal audit departments. Expectations from a number of stakeholders including audit committees, senior executives, and regulators continue to evolve, to supplement the emerging view of the internal audit profession.

The issuance of an annual audit opinion acts as an acid test as to whether audit coverage has been appropriate—can it be distilled into an opinion on the design and effectiveness of internal controls and the organization’s risk and control culture?

Reporting the annual audit opinion provides additional comfort to the board of directors regarding the organization’s system of internal controls. The work required to support annual audit opinion reporting should be considered as part of the annual audit needs assessment in order to ensure there is sufficient coverage and that it is prioritized appropriately.



Risk management

Risk appetite framework

Financial services organizations have continued to invest time and resources, particularly at the senior management level, in developing risk appetite frameworks during 2015, with many organizations requesting that their internal audit department conduct an audit of the risk appetite framework. Many internal audit departments have based these audits on the Principles for an Effective Risk Appetite Framework, published by the Financial Stability Board in November 2013. However, these organizations have found that the principles require a degree of interpretation and therefore many internal audit departments have required technical support to scope and execute such an audit. Typical findings from audits conducted during 2015 include failure to adequately demonstrate a linkage between the board level risk appetite statements and standards applied by the business, along with a lack of evidence relating to roles and responsibilities for risk appetite across the three lines of defense.

Insurance coverage

Directors' and officers' insurance coverage has a high profile at board level. With increasing focus from the regulators and other external bodies on the growing accountability of directors, boards of directors are seeking increased comfort that their insurance policies are going to operate effectively in the event the directors or officers of the organizations need to make a claim. It is important that the internal audit departments are able to challenge the processes in place to review the insurance-buying decisions made by the organization's in-house insurance function, and understand how the policies tie back to the organization's risk appetite.

Operational risk

As organizations continue to develop and fine-tune their operational risk assessment methodologies and taxonomies, thus building a richer picture of the potential risks, effective prioritization of risk mitigation comes into focus. This will become more crucial—especially in jurisdictions like the UK that introduce individual accountability requirements. Internal audit should incorporate an assessment of the quality of decision-making and extent of the risk mitigation activity by senior management.

Elements of the operational risk framework have often been developed and introduced as separate frameworks and methodologies (e.g., risk appetite, risk assessment, scenario analysis, issues management, loss data capture, etc.). Many organizations now face the challenge of integrating these elements into one coherent and dynamic framework. Without an integrated framework, the processes may not offer a practical solution to day-to-day risk management, and may not facilitate control environment improvement as expected by the regulators. Internal audit should assess the quality of linkages between the identification, assessment, mitigation, and monitoring/reporting stages of the risk management cycle.

Model risk

With the increasing use of complex quantitative models throughout the financial services industry, model risk has become a major concern for boards of directors, regulators, and external parties like insurers, banks, and investment managers. Model risk is largely the potential for inaccuracy and/or inappropriate use of models, which can lead to substantial financial losses and reputational damage.

The boards and regulators are particularly concerned about the materiality and magnitude of model error and its wider impact on the financial services industry. As a result, the regulators expect internal audit to have a strong focus on specialist regulation and technical concepts, particularly where models are used for regulatory purposes (e.g., capital adequacy). Internal audit should provide an independent evaluation of the effectiveness of model risk governance and controls, model risk appetite, and model risk identification in organizations. In order for internal audit to provide an independent assessment of the model risk framework, internal audit staff should ensure it has relevant subject matter expertise.



Regulatory matters

New regulators

Across the United Kingdom and Europe, several new regulators have joined the regulatory establishment. In the UK, the Payments Systems Regulator (PSR) aims to address concerns that have been raised about a number of issues in the payments industry, including access to the UK payments systems, the terms offered for access and the industry's pace of innovation. The PSR has already launched two reviews. Since April, the FCA and the UK's Competition and Markets Authority have been concurrent competition regulators for the financial services industry.

The European Union's supervisory architecture has also undergone major transformation, as two new banking regulators have assumed their powers—the Single Supervisory Mechanism (SSM), with the European Central Bank in charge, and the Single Resolution Mechanism (SRM), which is led by the newly established Single Resolution Board. Amongst its priority areas, the SSM is working on the validation of internal capital models, the calculation of risk-weighted assets, the reduction of discrepancies in prudential requirements across countries, and business model viability. The SRM expects to be fully operational from 2016.

This expansion of supervisors and responsibilities will raise regulatory activity and the interaction of regulators with organizations; it will also broaden the scope of activities that are under active scrutiny within a financial organization, leading to a greater demand on staff at organizations and likely expectations of higher standards at least in some areas. Supervisory relationships will become more complex and more challenging to manage. At the same time, there will be an increased benefit for organizations to getting things right first time, as well as monitoring for future priorities and areas of focus.

Retail conduct

In recent years, many financial services institutions have focused on embedding greater awareness and integration of retail conduct risk within their risk framework and appetite. There are increasing regulatory expectations that organizations are able to demonstrate that conduct-focused behavior and customer outcomes are truly embedded and play an integral part in all strategic and operational decisions.

Financial crime

Financial crime remains a key concern for regulators, as indicated by their continued supervision and enforcement activity. This long-term and continuing trend is evidence that organizations are still struggling with the basic requirement to establish appropriate systems and controls to identify and manage financial crime risk.

Organizations across the industry are at different stages of maturity with their financial crime arrangements and those potentially most at risk can often be the least prepared. There is an increased use of attestations as a supervisory tool. These trends are only set to increase with the adoption of the fourth EU Money Laundering Directive and with the introduction of additional supervisory techniques.

Financial sanctions continue to be a high priority for governments and financial organizations and so should be considered alongside other areas of crime prevention to ensure a holistic view of financial crime risk. Achieving this for some organizations remains a considerable challenge. Organizations may need to consider the adaptability of their financial crime arrangements (especially systems), given the frequent changes and amendments that are made to sanctions at an international, supranational, and domestic level.



Capital and liquidity

Solvency II

Starting on 1 January 2016, European Directive 2009/138/EC, which is known more commonly as Solvency II, sets out a step change in capital management, risk and governance frameworks, and regulatory reporting for all European insurers in its scope. Solvency II's main aim is to protect policyholders' interests by making insurers more resilient and less likely to fail, thereby reducing market disruption. Insurers have a choice to use a Standard Formula to calculate their capital requirements under Solvency II, or to produce an internal model which must be validated. These models are accompanied by the new Own Risk and Solvency Assessment, which is similar to the Individual Capital Assessment for UK insurers. There will also be public (Solvency and Financial Condition Report) and private (Regulatory Supervisory Report) reporting of the Solvency II results for organizations, including quarterly reporting to local regulators along with a new narrative reporting requirement for these reports.

Data quality

Data quality that is fit for purpose for capital and liquidity reporting allows financial organizations to maximize their value from data, whereas poor data inhibits the achievement of strategic goals and potentially exposes the organization to significant regulatory risks, operational challenges, loss of market competitiveness, and wasted costs. This can include incorrect CRD IV regulatory capital reporting (such as risk-weighted assets and capital ratios) that is not in line with filing rules and incorrect Value-at-Risk results for management oversight of the organization's capital. Furthermore, for

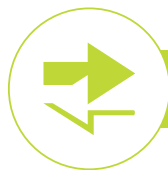
global systemically important banks, under BCBS 239, the requirement for effective data aggregation and risk reporting becomes effective in early 2016. BCBS 239 has specific principles focused on data quality and data governance, and as part of the governance principles, it sets out a requirement for ongoing independent validation of Risk Data Aggregation processes—i.e., internal audit should audit data quality.

Internal audit should play a pivotal role in enhancing the control environment and reducing the risk of poor data quality by conducting reviews of data quality processes. In addition, focused reviews of associated governance practices of data rich processes should be reviewed. Use of analytics in internal audit is an effective way to identify data quality issues in thematic reviews to ensure the data is of sufficient quality to get value from analytics.

Basel 3/CRDIV

The Capital Requirements Directive (CRD) IV implements Basel 3 in the European Union and prescribes rules covering capital, leverage, liquidity, corporate governance, and regulatory reporting. The new rules were applicable from 1 January 2014, subject to a number of transition points. Implementations for some of the capital and liquidity requirements are on a phased basis through 2019 and beyond.

CRD IV has led to increased expectations on internal audit. Increasing regulatory expectations around capital, liquidity, stress testing, and models result in higher demands on internal audit, both from regulators and from management.



Trading

Product & valuation controls

Product & valuation controls at many financial services organizations are not yet at the desired standard. This is often due to system infrastructure weaknesses, which remain the root cause of many control problems. The forthcoming prudent valuation regime, which is expected to be finally approved by the European Commission, will place further expectations on these organizations to produce and manage comprehensive data on the valuation risk of the organization, which can only be done effectively on top of a well-designed control environment. Identifying and challenging an organization's product & valuation controls should remain a key priority for internal audit over the next year. In addition, internal audit should also consider the organization's broader control activities, which contribute to the valuation controls, rather than just defining them narrowly as the independent price verification process.

Fair and Effective Markets Review (FEMR)

FEMR was established in the UK in June 2014 to conduct a comprehensive assessment of the way that wholesale financial markets operate in the UK. FEMR published its final report, setting out a range of recommendations to increase the effectiveness and regulation of the fixed income, currency, and commodity markets in the UK including promoting forward-looking conduct risk identification and mitigation. One of the earlier FEMR recommendations to be implemented was the expansion of the number of benchmarks under the FCA's supervision from one (LIBOR) to eight including SONIA, RONIA, WM/Reuters 4pm London Fix, ISDAFIX, London Gold Fixing, the LMBA Silver Price, and ICE Brent Index. The expansion of this oversight requirement extends the scope of internal audit to include review of relevant controls on a semi-annual basis.

FEMR was established in the UK in June 2014 to conduct a comprehensive assessment of the way that wholesale financial markets operate in the UK

Unauthorized trading

Significant unauthorized trading events remain a key risk area for many trading businesses due to the material financial and reputational impact that an event could have. The supervisory control frameworks at many financial services organizations have moved on significantly in recent years and are now well established, albeit continuing to evolve. Testing and confirming the ongoing effectiveness of these frameworks should remain a focus for internal audit.

High frequency and automated trading

The increasing use of high frequency and automated trading practices at many organizations increases their susceptibility to losses due to programming or other IT issues. For example, the volatile movement in the Swiss Franc exchange rates following its decoupling from the euro in January 2015 caused challenges for many organizations, which rely on automated hedging controls.

The compliance requirements of the Volcker Rule will increase for organizations caught in the scope of the rules. It is expected that Volcker Rule compliance will start to require an increasingly large allocation of the annual internal audit budget for those organizations with capital markets divisions.



Information technology

Cybercrime

An increasingly regular feature in the media over the past 18 months has been cybercrime, with multiple significant attacks and data breaches affecting all industry sectors, although financial services firms continue to bear the brunt. These upward trends demonstrate a fundamental shift in the nature of attacks, both in terms of complexity and persistence, driving a need for transformational change across the enterprise. High profile incidents, customers' concern, and media coverage are increasingly a compliance issue as well as a business one, with greater regulatory scrutiny, direction, and intervention than previously observed.

With the rise in breach size, impact, and complexity in 2015, incident response has seen a shift from a point-based 'fix-it' type approach towards a more holistic and sustainable one. Boards of directors and management are coming to the realization that they are not fully aware of the potential impacts of such breaches. This has necessitated more robust internal controls around incident response being embedded and integrated into the operational risk framework of a firm as a whole in order for it to remain responsive to these increasing impacts on businesses. It has also driven a need for businesses to systematically understand cyber risk at the board level. It is an opportunity for internal audit functions to demonstrate that they can understand and provide assurance over all the above. In addition, they should help promote increased organizational collaboration in cyber audits, both internally (between functions) and externally, as this will be a key area of focus for the sector over the coming months. This should enable a more transparent view of emerging risks and threats, and in turn drive more effective risk management practices while allowing internal audit to remain responsive to the changing nature of cyber threats.

IT disaster recovery and resilience

IT disaster recovery and resilience remains a key area of focus for financial sector organizations. IT system failures are increasingly front page news, leading to public coverage and reputational damage for a number of financial institutions. These failures rarely result in a full invocation of the disaster recovery and resilience plan for IT as they are more often a result of a management process issue or human error rather than a "big ticket" data center outage. Many progressive institutions are moving their focus from a traditional IT disaster recovery and resilience plan to a better understanding of the risks to services inherent in their IT environments (both in-house and at their external suppliers) and of the controls to mitigate them. These risks arise across technology, people, and processes. With this in mind, it is imperative that internal audit broadens its focus in the coming years to determine the adequacy of processes in place to avoid, respond, and recover from planned and unplanned outages.

Digital

Digital risks like mobile, cloud, and social media are interacting and converging. While this convergence holds the promise of new opportunities for organizations, digital also introduces new risks that may not be effectively managed by the organizations' existing governance, oversight, and internal control frameworks. A number of these risks were noted in the FCA's thematic review on mobile banking (September 2014), where financial institutions are using mobile banking as a catalyst for enhancing existing frameworks and future-proofing their digital risk landscape by having a better understanding of their digital footprint. Indeed, identifying, mapping, and truly understanding the organization's digital footprint will help internal audit have a more targeted and risk-focused view of the firm's digital landscape, which in turn can lead to a structured and robust plan for effectively auditing digital and unearthing the associated residual risks.



Continuous risk assessment

The recent explosion of data and management information can complicate and contradict the risk assessment as part of internal audit planning processes, if not managed effectively. This makes prioritizing and focusing audit planning and resources an ever greater challenge. Continuous risk assessment is a method of proactively identifying areas of potential risks through regular monitoring and measuring emerging trends in the risk profile of the organization. Use of analytics by internal audit functions can greatly enhance this process by identifying, measuring, and readily reporting such technology risks. Automation can provide measurement of these risks on a much more frequent basis. Visualization and dashboards can be developed for stakeholders to ensure they remain engaged and that results are clear and undisputable.

Furthermore, continuous risk assessment enables a rapid response to emerging risks, ensures the annual audit plan is continually aligned to risks, and allows for a more efficient use of resources by more precisely focusing on what matters. As well as audit planning, continuous risk assessment also supports tracking of audit actions. Simple and effective metrics can be used to demonstrate that control failures have been remediated, reducing the need for a full follow-up audit.

IT system failures are increasingly front page news, leading to public coverage and reputational damage for a number of financial institutions



Accounting and tax

Committee of Sponsoring Organizations (COSO) 2013 framework

Many financial services organizations applied the new COSO 2013 framework to their Sarbanes Oxley (SOX) controls for the first time in 2014. In 2016, the focus is building on the lessons learned by remediating the gaps identified and using the revision in framework as an opportunity to challenge and refine the universe of SOX controls over financial reporting.

Many financial services organizations applied the new COSO 2013 framework to their Sarbanes Oxley (SOX) controls for the first time in 2014

Tax risk management

Given ongoing fiscal challenges faced by governments in Europe, there continues to be significant political and media scrutiny over any aggressive tax avoidance and illegal tax evasion by those benefiting from and assisting such activities. Consequently, tax risk management continues to be a focus for financial services organizations wanting to ensure tax strategy remains fit for purpose and aligned with their broader commercial strategy and risk management approach.

In particular, banks with private banking businesses should have appropriately designed and effectively operating controls to prevent the bank from knowingly being involved in aggressive avoidance and tax evasion on behalf of their clients. Similarly, financial services organizations should have effective governance and supporting controls for their own tax exposure. Where the potential tax risk is material for the organization or its clients, internal audit should consider audits of tax governance and related controls to challenge their effectiveness.

Sources:

For the complete version, please visit Deloitte UK's website to download the publication that is also entitled Exponential change. Hot topics for internal audit in financial services for 2016.

Printed with permission by Deloitte UK





Clarity, transparency and comparability

The colors of the PRIIPs Regulation

Thierry Flamand
Partner
Insurance Leader
Deloitte Luxembourg

Florent Anders
Senior Consultant
Operations Excellence & Human Capital
Deloitte Luxembourg

Riccardo Rosa
Consultant
Operations Excellence & Human Capital
Deloitte Luxembourg



The Packaged Retail and Insurance-based Investment Products (PRIIPs) Regulation is a pillar of the EU's consumer protection normative framework, directly applicable in all EU Member States as of 31 December 2016. It focuses on products and requires clarity, transparency and comparability across them.

The KID (Key Information Document) is the instrument used to pursue this objective: a pre-contractual stand-alone document that informs investors on the investment in a timely and proper manner. Its three pages, structured in a question-based format, provide investors with answers to key questions.

On 9 December 2014, Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investments products (PRIIPs) (hereafter the Regulation) was published in the Official Journal of the European Union.

4 key questions:



WHAT IS
THE PRODUCT?



WHAT ARE
THE RISKS?

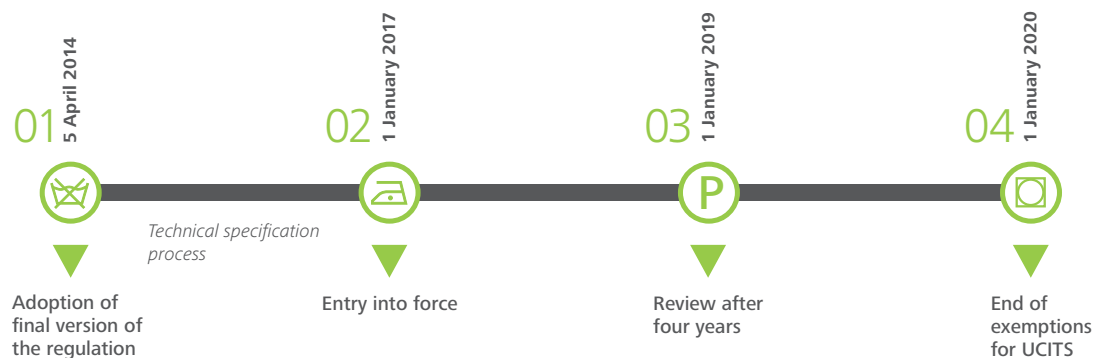


WHAT ARE
THE COSTS?



WHAT COULD
I GET IN RETURN?

The PRIIPs Regulation shall come into force on 31 December 2016



Context

The information provided to retail investors is sometimes misleading or not completely clear, making it difficult for investors to compare different products. Moreover, the conflict of interest between sales and the advice process may also lead to investments that are not in the best interests of the investor. Products may also not fulfil investors' needs, and investors may not always understand all product features and the risk linked to such investments.

To address investors' concerns and restore consumers' trust in financial products, the Regulation is designed to enhance the transparency and comparability of selected financial products through the issue of a standardized stand-alone disclosure document, the Key Information Document (KID).

The European Parliament moreover adopted the MiFID II package on 15 April 2014, to further improve investor protection. This package was designed to modernize MiFID, solve issues resulting from the financial crisis and thus foster a more efficient, resilient and transparent financial market. The PRIIPs Regulation and MiFID II complement each other: while the first focuses on disclosure requirements at product level, the latter targets investment advice. Only a few MiFID II provisions affect insurance-based investment products (within the scope of the PRIIPs Regulation) and amend the Insurance Mediation Directive (IMD), prior to the entry into force of the revised version, the Insurance Distribution Directive (IDD).

In another development for the EU consumer protection normative framework, 16 July 2015 saw the Council of the European Union publish the final agreed version of the text of the Insurance Distribution Directive (IDD), formerly known as the Insurance Mediation Directive 2 (IMD II). This amends and replaces the 2002 Insurance Mediation Directive (IMD I) and is expected to enter into force before the end of 2017, with a review to be carried out after five years.

IDD is designed to significantly raise the minimum standards of the IMD I and ensure a level playing field between all participants involved in selling insurance products, in order to achieve improved consumer protection, integration and competition. Its focus is prominent issues like intermediary qualification, advisory duty, remuneration and commissions, conflicts of interest and product design. The aim of the Directive is minimum harmonization; hence, it does not preclude Member States and national competent authorities from maintaining or introducing more stringent provisions, provided that these are consistent with its guidelines.

PRIIPs, MiFID II and IDD are the instruments required to realize a singular EU normative framework, with the aim of strengthening protection for consumers and investors from all of the different industries involved (e.g., banking, insurance, and fund/investment management) and standardizing each discipline as much as possible, with a particular focus on the clarity and transparency of marketed products.

Actors and products involved

All PRIIPs manufacturers are affected by the Regulation (e.g., fund managers, Insurers, credit institutions and investment firms).

For UCITS and investment management companies, the application of the PRIIPs provisions will not be mandatory until 31 December 2019, meaning that they can continue to provide KIIDs in accordance with Directive 2009/65/EC (UCITS IV). In light of both the significant investments made to implement KIIDs and the fact that the PRIIPs Regulation will pass through a review process four years after its entry into force, it is unlikely that UCITS will adopt the KID before the review.

With regard to products, the PRIIPs Regulation affects those offering investment opportunities to retail investors, where the amount repayable is subject to fluctuations because of exposure to reference values, or to the performance of one or more assets which are not directly purchased by the investor.

Such products include (non-exhaustive list):

- Guaranteed interest rate insurance contracts with profit-sharing schemes
- Unit linked products
- Investment funds
- Structured products (i.e., market-linked investments)

The following products are not in scope:

- Non-life insurance products as described in Annex I of Directive 2009/138/EC (Solvency II)
- Life insurance contracts where the benefits are payable only on death or in the event of incapacity due to injury, sickness or infirmity
- Deposits other than structured deposits as defined in Article 4 of Directive 2004/39/EC (MiFID)
- Securities as described in points (b) to (g), (i) and (j) of Article 1 (2) of Directive 2003/71/EC (Prospectus Directive)
- Pension products which, under national law, are recognized as having the primary purpose of providing the investor with an income in retirement and which entitle the investor to certain benefits

- Officially recognized occupational pension schemes within the scope of Directive 2003/41/EC (Occupational Pension Funds Directive) or Directive 2009/138/EC

Sanctions

Member States and competent authorities are responsible for establishing appropriate administrative penalties and measures applicable in the event of an infringement of the PRIIPs Regulation. They must also ensure they are properly implemented. Sanctions shall be effective, proportionate and dissuasive.

The conflict of interest between sales and the advice process may also lead to investments that are not in the best interests of the investor

The following list provides some examples of infringements (non-exhaustive list):

- The PRIIPs manufacturer not drafting a KID before the PRIIP is made available to investors
- The form and/or content of the KID not complying with the provisions
- The language of the KID not complying with the PRIIPs provisions on official languages and translation requirements
- The KID not being presented in the sequence/ layout defined by the Regulation or not containing all necessary information (e.g., name and type of PRIIP, objective(s) pursued and means to achieve them, specification of markets in which the product invests, summary risk indicator and possible maximum loss, performance scenarios, benefits and circumstances that trigger them, etc.)
- The marketing communications related to the PRIIP diminishing the significance of KID information or even contradicting it

With regard to sanctions, Member States may provide for additional sanctions or higher fine levels. However, competent authorities may impose the following as a minimum (non-exhaustive list):

- An order prohibiting/suspending the marketing of a PRIIP
- Administrative fines (minimum applicable) for legal entities:
 - Up to €5,000,000 or up to 3 percent of the legal entity's total annual turnover (based on the last available financial statements), or
 - Up to twice the amount of the profits gained or losses avoided because of the infringement, where those can be determined
- Administrative fines (minimum applicable) for natural persons:
 - Up to €700,000, or
 - Up to twice the amount of the profits gained or losses avoided because of the infringement, where those can be determined

KID: a standardized document with seven sections

The KID is a stand-alone disclosure document. It does not replace any other contractual documents, nor is it replaced by any of them.

The KID is divided into clearly defined sections: apart from the first two sections, which introduce the product through an overview of the investment and a brief description of the objective pursued, there are seven specific sections that each focus on a particular issue.





SECTION 1: "WHAT IS THE PRODUCT?"

In this section PRIIPs manufacturers must indicate the nature and main features of the product. The following information shall be necessarily present:

- *Type of PRIIP*
- *Purpose of PRIIP*, also indicating the means to achieve it, whether there is direct or indirect exposure to underlying investment asset, a description of the underlying instruments or reference values, the market(s) where the product invests in, as well as how the return is determined;
- *Intended market*, meaning the type of targeted retail investor, with specification of their investment horizon and ability to suffer from investment loss



SECTION 2: "WHAT ARE THE RISKS AND WHAT COULD I GET IN RETURN?"

In this section, PRIIPs manufacturers must describe the risk-reward profile of the product, including the following elements as a minimum:

- *Summary Risk Indicator* (i.e., the position of the product on a scale ranging from low risk to high risk), accompanied by a brief narrative explanation of the indicator and its main limitations, as well as a description of the risks that are substantially relevant to the PRIIP and those that are not sufficiently represented by the risk indicator
- *Performance scenarios*: manufacturers must also include, where applicable, the conditions for returns and/or performance caps, as well as a clear statement informing investors about the impact of the investor's home Member State tax legislation on pay-out



SECTION 3: "WHAT HAPPENS IF [NAME OF PRIIP MANUFACTURER] IS UNABLE TO PAY OUT?"

In this section, PRIIPs manufacturers must indicate whether the possible loss is covered by an investor compensation or guarantee scheme; if this is the case, they must also include the name of the guarantor, the type of guarantee scheme and the scope of covered risks (i.e., which risks are/are not covered).



SECTION 4: "WHAT ARE THE COSTS?"

In this section, PRIIPs manufacturers must indicate the costs over time and their composition: a breakdown of direct and indirect costs for the retail investor must be included, as well as a description of one-off and recurring costs. All of this information must be presented in the form of summary indicators.

Moreover, to ensure comparability across products, improve transparency and highlight the compound effect, total aggregate costs (i.e., performance fees, trailer fees, advisory fees, management and operating fees), must be expressed both in monetary and percentage terms.



SECTION 5: "HOW LONG SHOULD I HOLD IT AND CAN I TAKE MONEY OUT EARLY?"

The objective of this section is to clearly document the "Recommended minimum holding period" (expressed in years). In addition, PRIIPs manufacturers must also indicate, where applicable:

- The cooling off or cancellation period
- The opportunity for disinvestments before maturity, stipulating the conditions under which they are possible, as well as all fees and/or penalties applied
- The potential consequences of cashing in before the established term or the recommended holding period (i.e., loss of capital protection or extra fees borne by the investor)



SECTION 6: "HOW CAN I COMPLAIN?"

In this section, PRIIPs manufacturers must indicate how and with whom a retail investor can lodge a complaint about the product itself or the conduct of the PRIIP manufacturer or the person advising and/or selling it.



SECTION 7: "OTHER RELEVANT INFORMATION"

In this section, PRIIPs manufacturers must outline any other relevant information to be provided to the retail investor at a pre-contractual stage. Marketing materials, whatever their content, must be excluded.

Major challenges for PRIIPs

The PRIIPs Regulation will have a significant impact on distribution processes, as manufacturers must produce a KID for each of their PRIIPs and ensure that it is promptly provided to the investor prior to the investment. In this regard, dissemination is a key issue: investors must receive the KID in a timely manner prior to the investment, thus both manufacturers and distributors must identify the most suitable dissemination method (e.g., a dedicated website to be implemented and managed) and be able to prove that it was actually delivered (e.g., when required to do so by the authorities).

Management of volume, content and life-cycle will certainly require the allocation of dedicated resources or outsourcing to external specialized providers. Furthermore, in some cases the KID must be produced in addition to existing documents, such as an “encadré” or “nota informativa” for products offered to foreign residents.

Moreover, it will be necessary to define a compliance strategy for each type of PRIIP manager (manufacturer or distributor), which could include:

- An assessment of the effects on distribution processes (e.g., the review of SLAs between manufacturer and the distributor, which must be compliant with mutual responsibilities pursuant to the Regulation)
- The classification (KID positioning map) of all marketed products, primarily outlining the three key pillars of risk, cost and performance, with a view to ensuring investors always have a full picture of the range on offer

The compliance strategy will naturally entail a parallel evaluation of the skills and resources required to implement it, whether they are in-house resources and/or outsourced resources.

The KID will reflect industry-specific factors (for the banking, insurance and investment management industries). For instance, Insurers will face the challenge of drafting a reliable and exhaustive KID within an open architecture model where costs, risks and the performance of the associated underlying asset are not known in advance.

Nevertheless, for all stakeholders, the PRIIPs Regulation constitutes an important means of raising distributors’ level of awareness, knowledge and expertise (e.g., sellers will be required to respond promptly and properly to customers/investors’ questions on KID content, without delegating the responsibility to manufacturers).

In the main, the entire new EU framework constitutes a major opportunity to rethink and renovate processes, instruments and structures, in accordance with the emergence of new technologies, the evolution of customer preferences and the advent of new competitors.

The new provisions and the actions needed to implement them may also represent a boost for business digitalization, particularly in the case of outsourcing the production of KIDs. Deloitte Luxembourg, indeed, leveraging on its consolidated UCITS KIID production service offers an outsource solution for the production and life cycle management of the KID, covering content creation, document production, dissemination and web publishing.”



\$88.00



PSD2 opens the door to new market entrants Agility will be key to keeping market position

Stephen Ley
Partner
Risk Advisory
Deloitte UK

Steven Bailey
Director
Risk Advisory
Deloitte UK



The newly agreed Payment Services Directive 2 (PSD2) paves the way for significant changes to the payments market. This regulation needs to be carefully considered given its far-reaching impacts on how the market operates and not be treated as a straightforward compliance exercise. As at the end of October 2015, the regulation has been voted on and approved by the European Parliament and will shortly be formally adopted and published. Once this happens, EU Member States will have two years to implement the changes which can therefore be expected to come into force by the end of 2017.

Introduction

Following the vote to adopt the new Directive, the European Commission highlighted key parts of the new legislation in its press release: making payments throughout Europe safer and more secure, and enabling innovation by allowing new payment services to enter the market.

The drivers behind the regulation are clear: innovation, competition, and consumer protection. These are recurring themes that are being consistently pushed by regulatory authorities throughout Europe, both centrally and within its Member States.

The changes proposed by the PSD2 regulation are far-reaching. Set against a backdrop of increasing Fintech investment, PSD2 now enables many new third parties to participate in a market that has previously not been open to them. Existing players in the payments market must be responsive to the new challenges that this brings.

Overview

The original Payment Services Directive (PSD) was released in 2009 and put in place a legal framework for the Single Euro Payments Area (SEPA) for payments made throughout Europe. The aim of the PSD was to increase competition through new market entrants, improve payment efficiency, and reduce costs. The revised PSD2 has recently been agreed as a means to respond to changes in the payments landscape occurring since the original PSD was enacted.

PSD2 extends the original scope of the PSD and in particular increases the number of new entrants into the payments market, which in turn affects competition and increases the variety of payment services available.

PSD2 includes many new areas that bring into scope a number of new payment operators from gift card/loyalty schemes to account access services and mobile wallets.

The new regulation builds upon a number of areas within the original PSD, extending and clarifying some of the original articles and driving a higher focus on payments innovation, particularly in mobile. New areas of the directive include opening access to customer accounts and payment processing services.

Alongside PSD2, a second regulatory initiative (Regulation (EU) 2015/751) introduces a cap on interchange fees for card-based payments. Interchange fees are fees that are set by payment card schemes and are paid by the merchant's bank (acquiring bank) to the customer's bank, which issued their card (issuing bank). These payments are generally not visible to either merchants or consumers.

The focus of the Interchange Fee Regulation (IFR) is to remove "*direct and indirect obstacles to the proper functioning and completion of an integrated market for electronic payments, with no distinction between national and cross-border payments*".¹ It will have significant impact on many players in the existing cards market and is forcing banks and card schemes to reconsider elements of their operating models.

Key Changes

With a range of new banks and payment companies emerging, consumers are being provided with ever higher levels of convenience with respect to payment services. As these new companies access the payment systems and accounts of the more established financial institutions, responsibilities for key areas such as security, refunds for unauthorized payments and correct payment execution are becoming spread across the different players. This is leading to a lack of consistency in consumer offerings. This issue is addressed in PSD2, which brings these new organizations fully into scope.

¹ Source: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2015:123:FULL&from=EN>

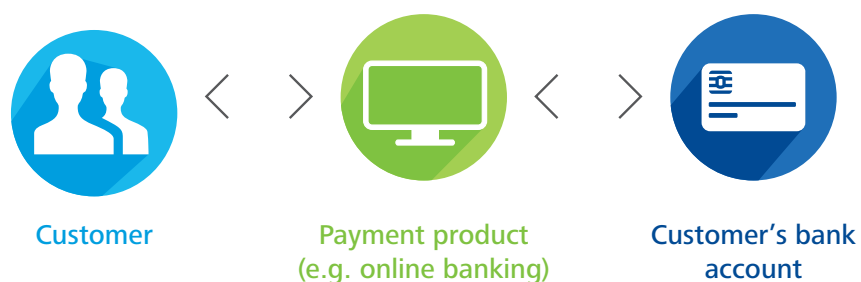


Some of the key changes enforced by PSD2 are described below:

1. Usage of Third Party Providers

Currently, the only way for customers to access their bank accounts to make payments is through products and channels provided by their bank, as shown below:

Current approach

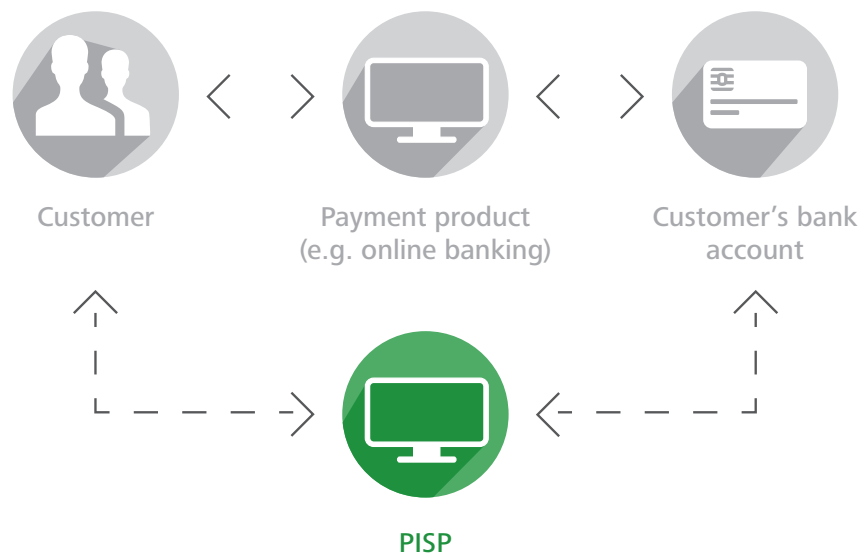


New areas of the directive include opening access to customer accounts and payment processing services

Under PSD2, two new types of Third Party Providers (TPPs) will emerge:

1. Payment Initiation Service Providers:

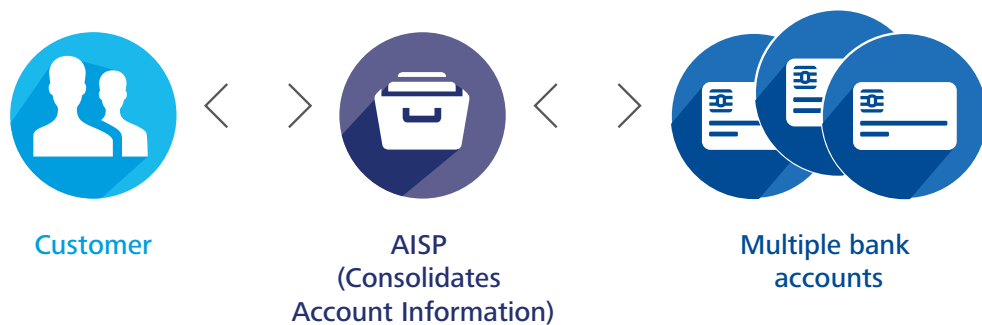
PSD2 will encourage competition in European payments by regulating Payment Initiation Service Providers (PISPs). Rather than the payer initiating the payment directly with their bank, the payer initiates the payment via the PISP, which in turn passes the instruction to the bank.



2. Account Information Service Providers:

These providers act as aggregators of customer payment account information. For example, presenting the Payment Service User (PSU) with an aggregated viewpoint of transactions and balances from more than one account. Currently, a PSU with more than one account would have to access each individually through a separate interface. Under PSD2, Account Information Service Providers (AISPs) are able to consolidate information from multiple accounts and present this back to the PSU.

AISP example



Of particular note, PISPs and AISPs will not be able to enhance their business model by using data captured during payment transaction processing, as the legislation forbids them to use this data for any other purpose than the provision of the payment service.

In addition, PSD2 defines traditional financial institutions that hold deposit accounts as **Account Servicing Payment Service Providers (ASPPS)**. In terms of pricing, PSD2 makes it clear that ASPPSs may not charge differently for payments initiated through the PISPs than they would for payments initiated by the PSU through their own systems.

The usage of TPPs provides consumers with additional options to access their bank, removing the need to interact with the bank directly. To enable TPPs to connect directly to a customer's bank, new technical standards are being developed by the European Banking Authority (EBA), which will define the connection requirements and API to be used. This is referred to as "Access to Account" or XS2A.

The usage of TPPs is the most significant change proposed by PSD2 as it alters the way payments can be made by a consumer. This in turn is expected to foster innovation and encourage new entrants to enter the payments market.

2. Security and Authentication Requirements

Security is a key component of PSD2 and the regulation introduces new security requirements covering account access and electronic payments. It also requires significant security requirements to be implemented by AISPs and PISPs. The security requirements build on the guidance already issued by the EBA in its Guidelines for the Security of Internet Payments².

The most significant requirement is for payment transactions to be subject to strong customer authentication. The EBA is responsible for the preparation of draft technical standards, which will define how security measures are implemented in practice under PSD2.

All Payment Service Providers (PSPs) including TPPs will need to ensure they can demonstrate adherence to the new security requirements. There is also a requirement for PSPs to provide to the competent authority a comprehensive assessment of the operational and security risks relating to their payment services on an annual basis.

3. Extension of scope

PSD2 includes in its scope "one leg out" transactions which are payments made to or from locations outside Europe. Whilst only the European parts of these transactions are caught, PSD2 aims to provide transparency over end-to-end charges and delivery terms.

Transactions that are made in non-European currencies will be captured under PSD2 where the PSPs for the payer and recipient are located in the European Union (EU). Transactions in any currency where one PSP is located in the EU and one PSP is located outside of the EU, will also be included within scope as "one leg out" transactions. These transactions were out of scope of the original PSD; the new regulation will therefore bring a large number of additional transactions within its remit.

PSPs will need to carry out an impact analysis and assess which parts of each transaction qualify as having been "carried out in the Union" and ensure adherence to the regulation for these segments.

Changes under the IFR

In December 2015, the IFR brings in caps on interchange fees of 0.2 percent and 0.3 percent of transaction value for debit cards and credit cards respectively. EU Member States will be able to enforce lower caps than those required by the legislation. Three party payment schemes that use PSPs as issuers or acquirers are covered by the regulation and will be allowed a transition period of three years as long as they do not exceed more than 3 percent of the market value of total card transactions on an annual basis. The compliance date for these three party schemes is expected to be December 2018 while other three party schemes are excluded from the regulation.

² <https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments>

The other major change enforced by IFR is that from June 2016, payment schemes and processors are required to be separated in terms of their accounting, organization and decision-making process. This significantly changes the operations of the schemes.

Impacts of PSD2

There are far-reaching impacts from the new regulation on all payment providers. In particular, there is an onus on the banks to ensure they adhere to the new requirements for access by third parties and for increased online and mobile security. They will have to deal with a number of new intermediaries as an additional layer between them and their customers. Whilst financial institutions will need to ensure they achieve compliance with new access and security requirements, the changes under PSD2 will also have a wider impact, encroaching upon payment revenue and introducing numerous competitors into the market. This must be carefully considered and will result in changes to commercial relationships and existing business models.

The impacts on specific parties are discussed below:

PISPs and AISPs

These newly defined TPPs under PSD2 will need to ensure they have structures in place to demonstrate appropriate compliance with the requirements of the regulation. For newer or start-up providers, this may entail significant changes to existing operating models. Other areas of consideration are listed below:

- Demonstrating compliance with the necessary security requirements for submitting payments is key area for TPPs. These requirements are likely to be extensive and will include obligations from both a customer authentication perspective as well as security over communications with ASPSPs
- The ability to prove that payment transactions have been executed appropriately and in line with regulatory requirements is key in the event of any disputes in respect of non-executed, defective or late payment execution

The usage of Third Party Providers provides consumers with additional options to access their bank, removing the need to interact with the bank directly

- From a data privacy perspective, TPPs must ensure that data collected is protected and be able to demonstrate it cannot be used for any purpose other than the provision of the payment service
- As with any new payment service, this is likely to be subject to an increased level of interest from fraudsters. New providers should be wary of this threat and ensure that they are able to comply with the stringent requirements on refunds in the event of unauthorized transactions occurring
- Resilience is another key area of relevance to new TPPs as PSD2 enforces strict rules on non-execution, defective, or late execution of payments

Banks

Banks need to consider their response from both a compliance and competition perspective, in terms of how they react to TPPs. The latter will require significant research and strategic planning. Of note, the regulation does not preclude banks from acting as TPPs and so banks may want to consider whether and how they wish to offer similar services to newer Fintech entrants.



Some of the other areas banks need to consider are listed below:

- Banks will need to adapt their current compliance mechanisms for PSD to build in any new requirements from the updated regulation. Risk and compliance impacts on products and operational functions will also need to be considered
- In the same way as for TPPs, one concern is around security risks and protection of sensitive customer data given interactions with TPPs. Whilst standards for access are still being drafted, clear attention needs to be paid to how these standards will work and what level of security protection will be provided

Banks need to consider their response from both a compliance and competition perspective, in terms of how they react to TPPs

- Additionally, from a security perspective, banks will need to ensure compliance with security requirements, including two-factor authentication for payment transactions and access to sensitive payment data. Whilst regulatory authorities in the majority of EU Member States have confirmed they will require banks to comply with the EBA Guidelines for the Security of Internet Payments, some Member States, including the United Kingdom, do not currently require this. For those that do not, a higher level of changes will be required by any banks that are not in compliance with these EBA Guidelines

- Also, of note for all Member States, the current EBA Guidelines only cover Internet payments. Other payment channels such as mobile will also need to be considered
- Resilience of payments is a recurring issue for many banks and further consideration should be applied to this area from the perspective of PISP and AISP connections to initiate payment
- Prioritization of payment requests from TPPs is also important. PSD2 is clear that these payments must not be treated with any form of discrimination compared with payments initiated directly by a bank. Banks must ensure they can demonstrate that appropriate and fair processing capacity is provided for these payment types.
- An impact analysis of “one leg out” transactions will also be required to ensure that the segments of these transactions performed in the EU are subject to PSD2
- Assessment and investigation of the inherent fraud risk from the opening up of access to PISP and AISP services

APIs

The EBA will release technical standards that will cover the interfaces between TPPs and ASPSPs. The level of detail of the interfaces’ specifications is as yet unknown. The EBA will, however, be required to consider:

- Strong authentication requirements and any exemptions based on the level of risk of payment services, recurrence of payment transactions and payment channels used
- Safety of PSU funds and personal data.
- Fair competition among PSPs and technology and business model neutrality
- Allowing the development of user-friendly and innovative means of payment
- Risk to specific devices and different transaction types, such as contactless
- Reviewing and updating the standards on a regular basis

- IT development will be required to provide TPPs with access to consumer accounts, and to differentiate between when an AISP accesses information and when the PSU accesses information

ASPSPs will be required to:

- Ensure they communicate securely with PISPs.
- Make all required information immediately available to a PISP after receipt of a payment order.
- Treat payment orders from PISPs without any form of discrimination.

ASPSPs may deny PISPs and AISPs access to payment accounts for objectively justified and evidenced reasons related to unauthorized or fraudulent access to the account by the PISP or AISP. In these cases, the ASPSP must immediately report the incident to the competent authority and also notify the payer before access is denied, if this is possible, or at the latest immediately after.

IFR impacts

As well as the card schemes that will need to separate their processing capability, card issuers in particular are likely to be significantly affected by the reduction in interchange fees and will need to consider how existing business models and pricing strategies will adapt to the regulation.

Cross-border acquiring could also be impacted if some EU Member States set lower levels of interchange fee than the imposed caps. This may disadvantage overseas acquirers if domestic rates in a particular country are lower.

Conclusion

The amount of change that is coming through PSD2 is very significant and clearly has the ability to alter the payments market in a number of ways for the consumer and current market participants. There are major underlying impacts for existing market players from a strategy and competition perspective, as well as a higher compliance burden that will be enforced on all new and existing payment players.

New providers face an exciting challenge, as they are able to enter the market without access restrictions but should not underestimate the requirements of the regulation and the burden in being able to actively demonstrate compliance.

For well-established market participants, the ability to be agile in response to PSD2 and adapt services to counteract increased competition is key to ensuring market position is maintained.



Solvency II and key considerations for asset managers

Thierry Flamand
Partner
Insurance Leader
Deloitte Luxembourg

Xavier Zaegel
Partner
Financial Risks Leader
Deloitte Luxembourg

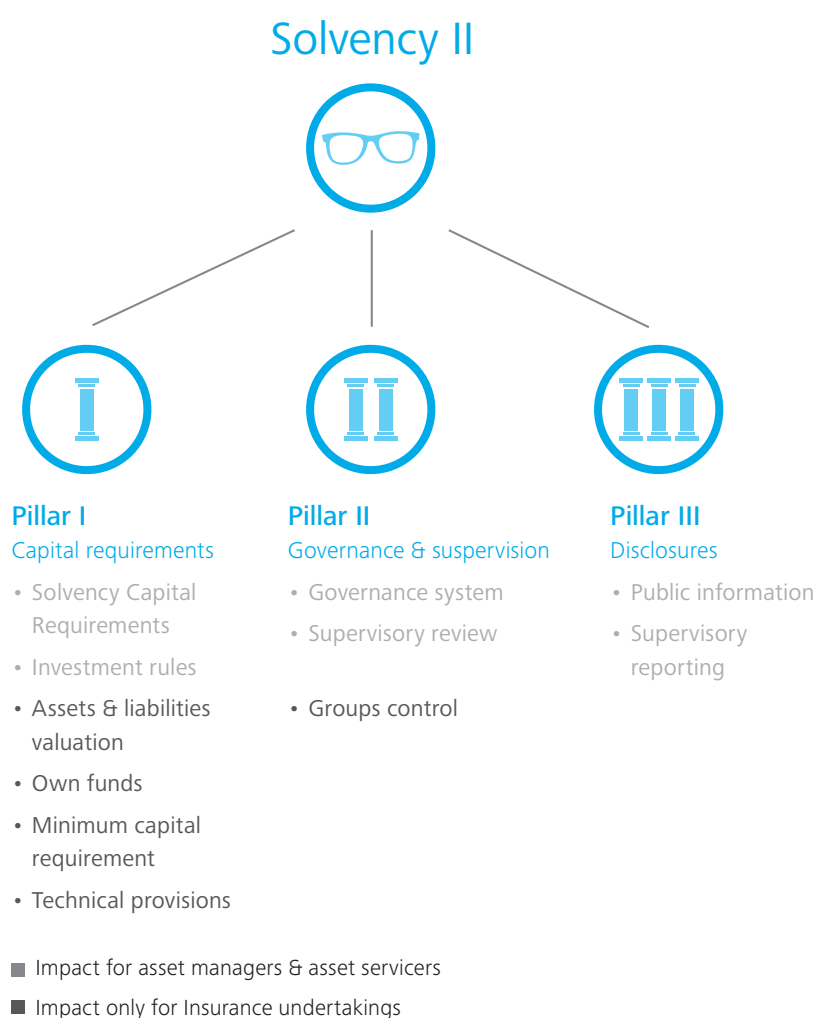
Sylvain Crepin
Director
Financial Risks
Deloitte Luxembourg

Michael Cravatte
Director
Insurance
Deloitte Luxembourg

With transparency as one of the key objectives of the Solvency II Directive, look-through demands from insurance/reinsurance undertakings will increase following the implementation of Solvency II. It will also add pressure on asset managers to make further progress with regard to data quality, governance and disclosure.

Well-prepared asset managers that offer Solvency II adapted products and reporting could gain a competitive advantage.

In terms of risk factors, market risk is expected to have the largest impact, between 50 and 75 percent of the final SCR according to a recent EIOPA study



1. Solvency II – A key milestone for the insurance and reinsurance industry

The Solvency II Directive, which has come into effect on 1 January 2016, is a harmonized, risk-based supervisory framework for insurance and reinsurance undertakings in the European Union.

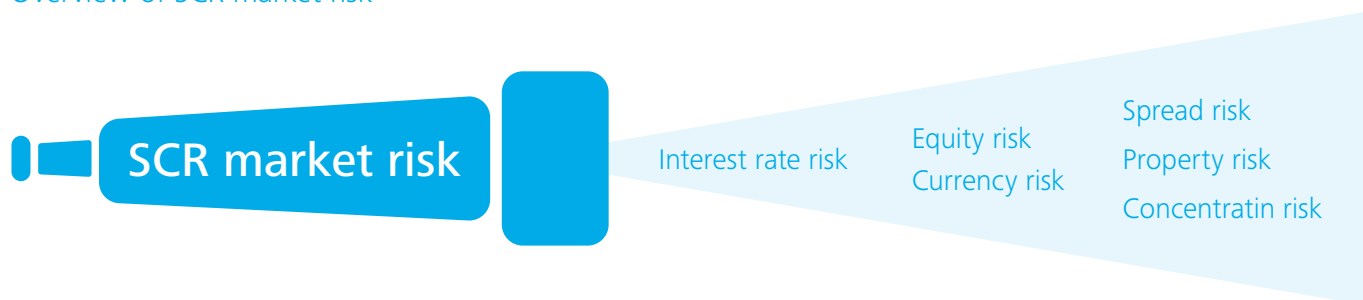
As per other financial services legislation, such as the Basel III framework for banking supervision, Solvency II has been organized in three pillars: Pillar I focuses on Solvency Capital Requirements (SCR), Pillar II centers on governance and supervision, and Pillar III addresses disclosure and supervisory reporting.

Unlike other regulatory frameworks, Solvency II stipulates that the calculation of Solvency Capital Requirements is based on a delta net asset value approach.

The insurer's assets and liabilities are subject to stress tests with pre-defined shocks set by the supervisory authority. Changes in net assets are combined with correlation matrices to derive the solvency capital requirement. Risk factors include market, health, default, life, non-life, intangible and operational risks, which makes it a complex and data-rich computational process.

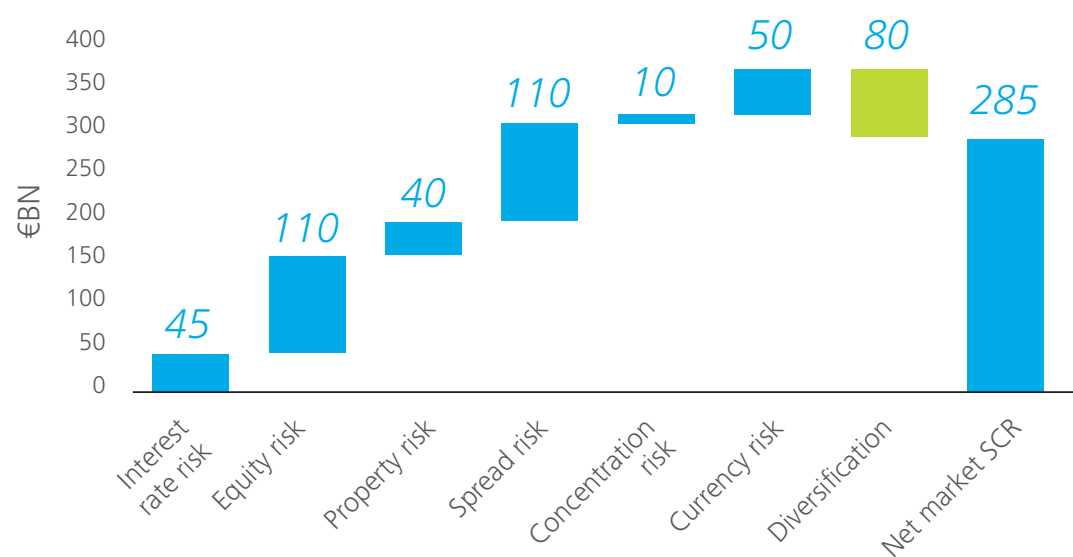
In terms of risk factors, market risk is expected to have the largest impact, between 50 and 75 percent of the final SCR according to a recent study from the European Insurance Occupational Pensions Authority (EIOPA). SCR market risk is derived from six sub-risk factors displayed below. Within market risk, equity, spread, currency and interest risks have the biggest impacts on the SCR.

Overview of SCR market risk



Market risk SCR decomposed

Core sample



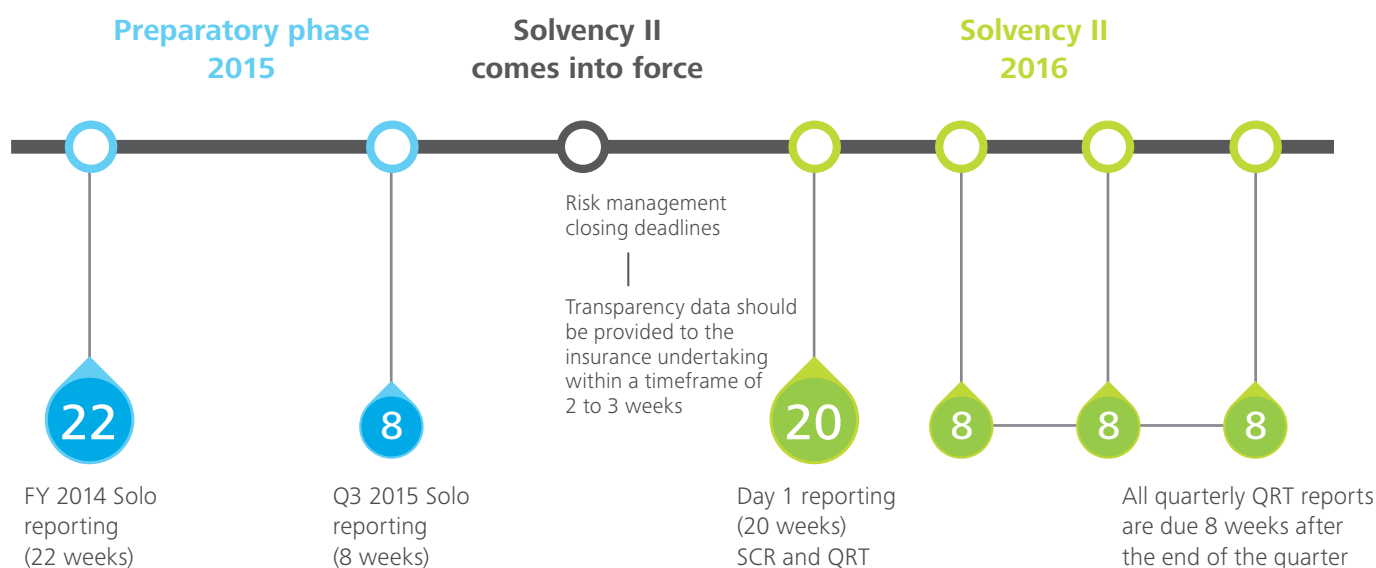
Source: EIOPA Insurance stress test 2014, 28 November 2014, SCR market risk decomposed

Reporting and timeframe

Insurance undertakings will have to provide the first set of Solvency II reports to their home state regulators in May 2016 and on a quarterly and annual basis thereafter (see graph below), with two main elements:

Solvency Capital Requirement and the Quantitative Report Template (QRT) on assets and liabilities. Notwithstanding regulatory obligations, some insurance companies may be tempted to estimate their Solvency Capital Requirements on a more frequent basis.

Regulatory reporting timeline within Solvency II

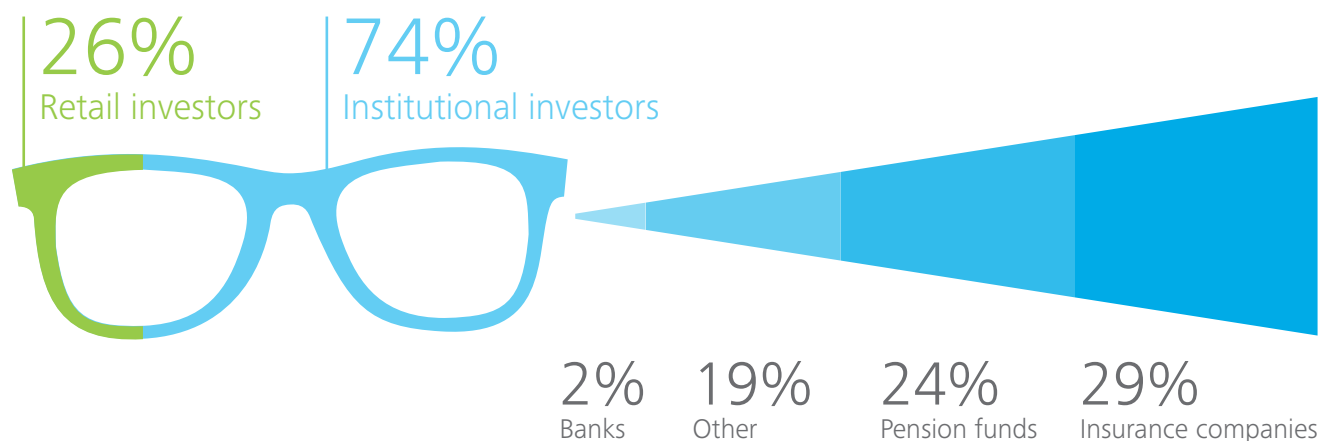


2. Solvency II and the look-through principle will change the way insurance companies work with asset managers

Insurance undertakings are key institutional investors for the asset management industry

Insurers are the largest institutional investors in investment funds, with an overall share in total European AuM of 29 percent, followed by pension funds at 24 percent.

Ownership of European investment funds



Source: Efama, Asset management in Europe, 9th annual review

A recent survey of 56 decision-makers in the German insurance industry shows that 72 percent intend to outsource much of their asset management to external providers following Solvency II. This percentage is even higher for smaller insurance undertakings.

Insurance companies have high expectations of asset managers in terms of reporting and disclosure

One of the main improvements of the Solvency II framework is the requirement to adopt a “look-through” approach in order to obtain an accurate picture of the risks with regard to assets and liabilities. As the management of a large proportion of insurance companies' assets (when not all of them) is outsourced to external asset managers through segregated accounts or units of collective investment undertakings, the assistance of the latter will be key in helping the former to perform the required look-through.

The assistance expected from asset managers mainly includes:

- Performance of a full look-through on portfolio investments for market SCR calculation and QRT reporting
- Estimation of risk sensitivities required for SCR calculations at investment or fund level

As the relationship between an insurance undertaking's assets and liabilities must be considered to underpin the market SCR of the insurer, it is not possible for asset managers to pre-compute the market SCR only based on their assets or a proportion of them. Asset managers may only use sub-modules of market SCR as a risk/performance indicator or as an indication of possible matches with specific profiles of an insurer's expected cash-flow obligations.

However, regarding unit-linked products, for which insurance companies do not bear the associated investment risks, market SCR calculated at fund level by asset managers may be used directly by

insurance undertakings in their SCR calculations, via the estimated revenue losses under the prescribed market shocks. As a result, insurance companies may look at investment funds' market SCR to compare the regulatory costs associated with them when packaged into unit-linked products. Calculating this risk indicator in compliance with Solvency II rules and the ability to provide appropriate assurance will become additional differentiating factors for the investment fund industry.

Indeed, 83 percent of survey respondents indicated that they had high or very high expectations of asset managers in terms of reporting and disclosure.

Facing rising operating costs and capital requirements, one may also expect insurance/reinsurance undertakings to undergo significant changes in their investment allocation strategies. Among the German insurance companies surveyed, up to 49 percent said they will reduce the number of external asset managers they use.

In conclusion, offering data and analytics reporting to insurance companies will no longer be just a compliance variable but a component in retention and acquisition.

Among the German insurers surveyed, up to 49 percent of respondents said that they will reduce the number of external asset managers they use



Data exchange timeline and frequency

Data and analytics exchanges between fund managers and insurance companies should be expected on a quarterly basis, but annual reporting might be an option for insurance companies that invest less than 30 percent of their portfolio in investment funds.

Insurance companies will submit reports to the supervisory authority four to eight weeks after the end of the quarter, which gives asset managers between one and two weeks to deliver the look-through data required by their insurance undertaking clients.

Among the German insurance undertakings recently surveyed, only 42 percent believe that their main asset manager will be able to submit the vast quantity of data in time.

Challenges associated with importing, enriching, classifying and computing data

One of the challenges associated with Solvency II reporting for asset managers and insurance undertakings is working with data files from different

sources with heterogeneous contents and formats. Data harmonization, enrichment of all securities with information from different data vendors, classifications of securities and computational analytics are also challenging.

In terms of data demands for asset managers, up to 100 items need to be collected per investment line from internal and external sources including details of derivatives and structured products that are not readily available. Additionally, appropriate data governance must be implemented to address data licensing and confidentiality issues as well as potential conflicts of interest.

In terms of analytics, between 10 and 50 sensitivities may be necessary to appropriately model a portfolio for SCR calculation purposes. This triggers the issue of portfolio compression and risk clustering if the insurance undertaking prefers not to provide (or receive) analytics and static information at instrument level in order to reduce the pressure on the undertaking's Solvency II system.

Among the German insurance undertakings recently surveyed, only 42 percent believe that their main asset managers will be able to submit the vast quantity of data in time

3. Asset managers joining forces to meet Solvency II reporting requirements

To help bridge the gap between data requirements and accessibility, and to encourage a unified approach throughout the industry, associations representing investment management professionals in France (AMPERE, AFG), Germany (BVI) and the UK (IA) have developed a common data exchange template (dubbed the Tripartite Solvency II reporting template or TPT) to support the demands of the Solvency II Directive. The TPT is structured so as to capture data required for Pillar I and Pillar III purposes (SCR calculation and QRT reporting), for which a look-through is expected on asset data.

Identification, optional and control information has also been included. The relevant information categories are as follows:

- Portfolio characteristics and valuation
- Instrument codification
- Valuation and exposure
- Instrument characteristics and analytics
- Transparency
- Indicative contributions to SCR for market risk
- Specific data for convertible bonds
- Specific data in case no reference yield curve is available
- Additional information

An updated 3.0 version of the TPT was released on 13 October 2015 with the support of EFAMA, Austrian, French, Luxembourg, Italian and Dutch fund and asset management associations.

The Tripartite Solvency II reporting template is widely used in France, the United Kingdom and Germany, and in more and more European countries.

Nonetheless, there are still several insurance companies which require a dedicated data format for all information relating to Solvency II, as they are not equipped to handle any other format.

Portfolio compression and data aggregation

One of the major issues for insurance companies pertaining to look-through on investment funds is the large volume of data received from asset managers. This requires significant data management capacities and efficient systems to perform the calculations required under Solvency II. However, insurance companies' Solvency II systems may not be able to handle thousands of portfolios and hundreds of thousands of investment lines, even when the information is presented in a harmonized format.

Some will prefer full disclosure of holdings whereas others will opt for minimal disclosure, and reporting of compressed portfolios structured around a small number of points which mimic the risk implications of the real portfolio. This is done with a view to reducing data processing workload and computation time.

4. Leveraging Solvency II with strategic portfolio considerations and new allocation strategies

While not meeting Insurance undertakings' transparency requests could potentially lead to a loss in market share, the new Solvency II rules mean that there is no guarantee that data reporting alone will suffice to preserve existing market share. Therefore, if not already approached, asset managers are encouraged to engage with their insurance undertaking clients to understand in more details how their investment products may interact with their liabilities and Solvency Capital Requirements. Understanding these dynamics may drive strategic changes for asset managers.

To return to the main underlying principles of the new regulatory regime and some of its strategic goals, one can expect an increasing proportion of insurance companies' assets to be allocated to long-term investments in the real economy targeting in particular SMEs and infrastructure projects, a reduction of complexity and an improvement of asset quality. Asset managers can anticipate these outcomes by structuring infrastructure and private equity funds and reducing the use of complex derivatives, securitizations and structured products.

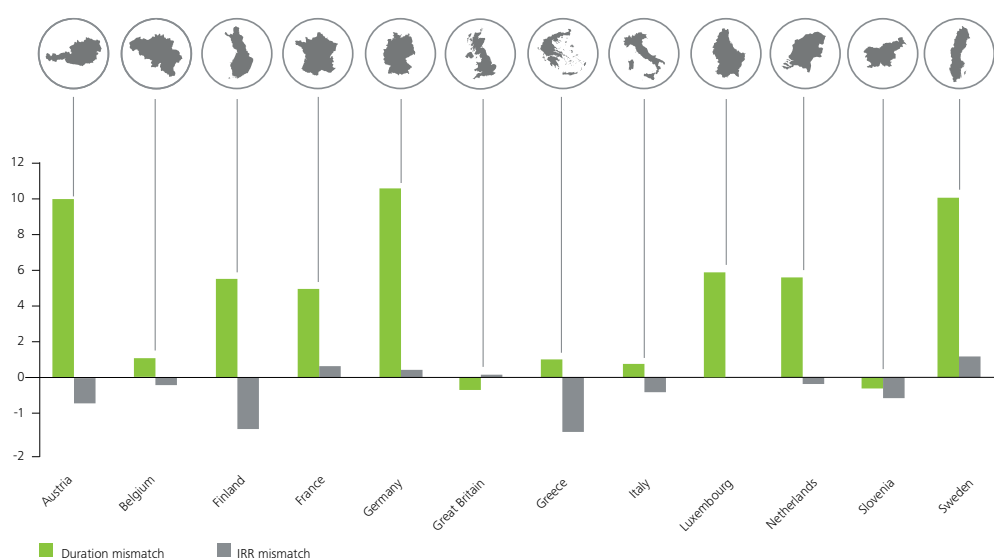
However, certain principles, such as matching the duration of assets and liabilities or matching cash-flows, may require a two-way communication channel to be opened, allowing asset managers to gain additional knowledge on insurance undertakings' specific needs or specific risk exposure and adjust or structure an investment product accordingly. This would result in a reduced solvency capital requirement for the insurance undertaking.

The Tripartite Solvency II reporting template is widely used in France, the United Kingdom and Germany, and in more and more European countries

A recent EIOPA study highlighted the broad duration and return mismatches of assets and liabilities for European insurance companies (see below), and estimated that up to 24 percent of companies would not meet their SCR under a continuation of current low-yield conditions. Long durations on the asset side remain difficult to source, with an average duration of five years for corporate bond investments and eight years for government bond investments held by European insurance companies (source: EIOPA stress test, 2014). High performing assets typically exhibit low duration (for example, this is true of high-yield bonds and corporate loans), or no duration at all (e.g., equities). EIOPA concluded that the continuation of the current low-yield environment could trigger significant issues for insurance companies in meeting promises to policyholders in eight to eleven years.

Insurance companies' ongoing need for asset performance and low Solvency Capital Requirements will require a closer dialogue between Insurers and the asset management industry.

Investment return and duration mismatches for European insurance companies



Source: EIOPA Insurance stress test 2014, 28 November 2014

In a nutshell:

- Solvency II has come into force on 1st January 2016 and insurance undertakings will submit their first regulatory reporting and disclosures in the next months
- Solvency Capital Requirements within Solvency II are based on a "look-through" approach on assets and liabilities and a "delta Net Asset Value" considering several risk factors
- Market Risk is the main driver of Solvency Capital Requirements, and essentially flows from the investment portfolios of insurance companies, very often outsourced to external asset managers
- Regulatory disclosures within Solvency II include a broad range of information on the asset mix of insurance companies and also based on a look-through approach for collective investment funds
- Insurance companies will therefore rely heavily on asset managers for providing them with transparency data and risk information on their investment products and portfolios
- European investment management associations led by the French Club Ampere have developed a common data exchange template (dubbed the Tripartite Solvency II reporting template or TPT) to support the demands of the Solvency II Directive to asset managers
- Beyond portfolio and risk transparency, Solvency II is expected to drive significant changes in the way insurance companies and asset managers work together

Note: mismatches in this table are calculated as the difference between the Internal Rate of Return (IRR) and the durations of liabilities minus those of assets. Therefore a negative mismatch implies higher IRR or duration for assets than for liabilities based on the cash flow reported by the participants to the EIOPA stress test on a country basis.



Transactions and Trade Regulatory Reporting *A changing landscape*

Simon Ramos
Partner
Advisory & Consulting
Deloitte Luxembourg

Laurent Collet
Partner
Advisory & Consulting
Deloitte Luxembourg



The implementation of the EMIR reporting, contrary to expectations, has probably been one of the most challenging reporting issues faced by market participants over the last years.

Buy side and sell side financial participants, as well as corporate participants, have had to take on an additional operational burden mainly due to the unexpected complexity of transposing roughly 80 transaction fields into Trade Repositories on a daily basis.

The market players were not accustomed to these daily reporting obligations, which were further impeded by the grey area around key reporting fields. The possibility of delegating the reporting to sell side brokers was therefore welcomed by the buy side. However, for those using multiple brokers and venues, delegating the reporting is not a silver bullet for solving all reporting requirements.

For more and more financial counterparties, the question is now how to put a long-term strategic transaction reporting solution in place

Furthermore, in EMIR - contrary to the Dodd-Frank Act (DFA) - each counterparty remains responsible to their regulator for ensuring timely reporting and accuracy of the data. Accuracy still remains a key issue when it comes to EMIR, partly because of the poor quality of some of the basic data being reported - namely the 'I' trio, i.e. the LEI, UTI, UPI fields. These challenges explain most of the reconciliation issues and the difficulties faced by reporting entities.

The European Securities and Markets Authority (ESMA) has decided to address the reporting issues with new validation rules which entered into force in November 2015 and are being applied by the Trade Repository.



ESMA is also addressing the need for clarification on some data fields and introducing a set of new fields related to collateral, Credit Default Swap (CDS) and new energy data in order to be aligned with the recent REMIT regulation for the energy market (Regulation on Wholesale Energy Markets Integrity and Transparency), which entered into force in October 2015.

Hand in hand with other future regulatory reporting requirements

In addition to the EMIR-related changes, the transaction reporting requirements will continue to pave the regulatory reporting highway in Europe and beyond within the next coming months and years.

MiFID II and MiFIR will extend the scope of EMIR with additional product types in the reporting scope. Transactions will be sent on a daily basis to the National Competent Authority (NCA) by the investment firms via the regulated trading venues or appointed reporting mechanism (ARM). MiFID II will also bring trade transparency to a wide range of financial instruments. ESMA estimates that the current data collection under MiFID I represents 10 percent of the volume that will have to be collected under MiFID II.

The Securities Financing Transactions (SFT) Regulation was adopted in November 2015. The financing transactions including repurchase agreements, securities or commodities lending/borrowing and buy-sell back or collateral swap transactions are to become reportable by financial and non-financial counterparties to the trade repository as from 2017.

Firms need to define a proper and long-term strategic trade transaction reporting model

For more and more financial counterparties, the question is now how to put a long-term strategic transaction reporting solution in place. EMIR and the upcoming transaction reporting regulations such as MiFIR and SFTR are seen as catalysts for reshaping the regulatory reporting processes. Indeed, these pre- and post-trade and transactions reporting requirements will be embedded in day-to-day operations and need to be properly supported by an efficient, reliable and scalable reporting IT infrastructure, operational processes and resources.

The design of the regulatory reporting model should not be organized as a set of different interfaces built around each regulation. Rather, it should be built around your trade and post-trade value chain, extracting the data from different applications and centrally consolidating it.

A well-designed transaction reporting model is the only way to achieve proper efficiency and consistency in data reporting and will furthermore give an organization a holistic view of the reporting compliance duties and will help establish a data repository infrastructure that meets multiple regulatory requirements.

New internal or outsourced reporting solutions will need to act as integrated platforms. These platforms should help regulated entities to achieve compliance on a cross regulation and cross-jurisdiction basis. According to recent studies, managed transaction reporting services can provide substantial cost savings and could be a valid alternative to in-house development.

The new transaction and trade reporting regulations (MiFID II and MiFIR) offer a unique opportunity for financial institutions to take a step back and review their current reporting strategies. It is time for regulated entities to question whether or not it makes financial sense to continue to adjust and adapt internal infrastructures, operations and resources, or if it would now make more sense to outsource trade reporting services.

A well-designed transaction reporting model is the only way to achieve proper efficiency and consistency in data reporting

Contacts

Australia



Timothy Oldham
Partner
+61 293 225 694
toldham@deloitte.com.au

Austria



Dominik Damm
Partner
+43 153 700 5400
ddamm@deloitte.at

Belgium



Arno De Groote
Partner
+32 280 024 73
adegroote@deloitte.com

Brazil



Luiz Dias
Partner
+55 115 186 6206
luizdias@deloitte.com



Elias Zoghbi
Partner
+55 115 186 6469
eliaszoghbi@deloitte.com

Canada



Bruno Melo
Partner
+1 416 601 5926
brmelo@deloitte.ca

Caribbean Bermuda Countries



Lawrence Lewis
Partner
+1 242 302 4898
llewis@deloitte.com

Central Europe



Andras Fulop
Partner
+36 1 428 6937
afulop@deloitteCE.com



Adam Kolaczyk
Partner
+48 225 110 858
akolaczyk@deloitteCE.com

CIS



John Roberts
Partner
+749 578 706 00
jorobarts@deloitte.ru



Julia Brovkovitch
Director
+749 578 706 00
jbrovkovitch@deloitte.ru

Colombia



Elsa Mena
Partner
+57 142 620 60
emenacardona@deloitte.com

Cyprus



Panicos Papamichael
Partner
+357 223 608 05
ppapamichael@deloitte.com

Denmark



Thomas Brun
Partner
+45 30 93 6571
tbrun@deloitte.dk

East Africa



Julie Nyangaya
Partner
+254 204 230 234
jnyangaya@deloitte.co.ke

Finland



Lasse Ingström
Partner
+358 207 555 389
lasse.ingstrom@deloitte.fi

France



Laurence Dubois
Partner
+33 1 40 88 28 25
ladubois@deloitte.fr

Germany



Jörg Engels
Partner
+49 211 877 223 76
jengels@deloitte.de



Christian Haas
Partner
+49 697 569 565 07
chaas@deloitte.de



Dr. Andreas Knaebchen
Partner
+49 152 090 076 00
aknaebchen@deloitte.de

Greece



Alithia Diakatos
Partner
+30 210 678 1100
adiakatos@deloitte.gr

Hong Kong & China



Tony Wood
Partner
+852 285 266 02
tonywood@deloitte.com.hk

Iceland



Sif Einarsdottir
Partner
+354 580 3009
sif.einarsdottir@deloitte.is

India



Muzammil Patel
Senior Director
+91 22 6185 5490
muzammilpatel@deloitte.com

Ireland



David Kinsella
Partner
+353 141 725 29
davkinsella@deloitte.ie

Israel



Naama Rosenzweig
Director
+972 3 608 5251
nrosenzweig@deloitte.co.il

Italy



Mariano dal Monte
Partner
+39 063 674 9293
mdalmonate@deloitte.it

Japan



Masayuki Tanabe
Partner
+81 908 349 3699
masayuki.tanabe@tohatsu.co.jp

Korea



Young Sam Kim
Partner
+82 266 761 522
youngskim@deloitte.com

Latin America Countries



Martin Carmuega
Partner
+54 11 432 027 00
mcarmuega@deloitte.com

Luxembourg



Laurent Berliner
Partner
+352 451 452 328
lberliner@deloitte.lu

Malta



Steve Paris
Partner
+356 234 324 00
stparis@deloitte.com.mt

Mauritius



Peter Manju
Partner
+230 403 5818
mpeter@deloitte.com

Mexico



Carlos Perez
Partner
+52 55 5080 6444
caperez@deloittemx.com

Morocco



Fawzi Britel
Partner
+212 661 154 586
fbritel@deloitte.com

Middle East



Aeja Ahmed
Partner
+966 1 282 8400
aeahmed@deloitte.com



Fadi Sidani
Partner
+971 437 688 88
fsidani@deloitte.com

Netherlands



Harmen Meijnen
Partner
+31 882 884 258
HMeijnen@deloitte.nl

New Zealand



Rodger Murphy
Partner
+64 930 307 58
rodgermurphy@deloitte.co.nz

Norway



Sverre Danielsen
Partner
+47 232 798 43
sdanielsen@deloitte.no

Portugal



Sandra Carla Martins
Associate Partner
+351 21 042 7506
smartins@deloitte.pt

Singapore



Tse Gan Thio
Partner
+65 6216 3158
tgthio@deloitte.com

South Africa



Akiva Ehrlich
Director
+271 180 661 75
akehrlich@deloitte.co.za

Spain



Alfonso Mur
Partner
+34 914 432 103
amur@deloitte.es

Sweden



Marcus Sörlander
Partner
+46 752 462 463
msorlander@deloitte.se

Switzerland



Sven Probst
Partner
+41 58 279 6401
sprbst@deloitte.ch

Taiwan



Thomas Wan
Partner
+866 225 459 988
thomaswan@deloitte.com.tw

Thailand



Somkrit Krishnamra
Partner
+66 2676 5700
somkrishnamra@deloitte.com

Turkey



Cüneyt Kırklar
Partner
+90 212 366 604 8
ckirlar@deloitte.com

United States



Scott Baret
Partner
+1 212 436 5456
sbaret@deloitte.com



Alok Sinha
Principal
+1 415 783 5203
asinha@deloitte.com

United Kingdom



Julian Leake
Partner
+44 207 007 1223
jleake@deloitte.co.uk

West and Central Africa



Anthony Olukoju
Partner
+234 190 417 39
aolukoju@deloitte.com

Contacts

**Rick Porter**

Partner
Deloitte US
Global Enterprise Risk Services Leader
Financial Services
Deloitte Touche Tohmatsu Limited
+1 312 486 2046
rickporter@deloitte.com

**Laurent Berliner**

Partner
Deloitte Luxembourg
EMEA Enterprise Risk Services Leader
Financial Services
+352 451 452 328
lberliner@deloitte.lu

**Scott Baret**

Partner
US Banking & Securities Leader
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Please do not hesitate to contact
your relevant country specialists
listed in the magazine

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.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see <http://www2.deloitte.com/global/en/footerlinks/about-deloitte.html> www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, 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 more than 220,000 professionals are committed to becoming the standard of excellence.

For the convenience of the reader, a member firm of DTTL in a particular country is identified in the body of this report by the word "Deloitte" coupled with a country name (e.g., Deloitte UK), in lieu of using the actual legal name of the member firm of DTTL in that country. In many countries, services may be provided by the actual member firms but could also be provided in addition by—or solely by—subsidiaries or affiliates of the DTTL member firm in that country, which are often organized as separate legal entities.

Specifically, with respect to the United States, Deloitte LLP is the member firm of DTTL and does not provide services. Services in the United States (U.S.) are provided by Deloitte LLP's subsidiaries; including Deloitte & Touche LLP, Deloitte Tax LLP, Deloitte Consulting LLP, and Deloitte Financial Advisory Services LLP. All of these U.S. entities are referred to in this publication as "Deloitte US." Certain services may not be available to attest clients under the rules and regulations of public accounting.

