

Realising the full value of compliance

Protecting the brand 2009

Executive summary



Contents

	<i>page</i>
Foreword	1
About this report	2
Executive summary	4
Reflections on the results of the study	
<hr/>	
The most challenging compliance risks faced by financial institutions	8
Enhanced focus on regulatory risk management	
Rebuilding customer trust	
<hr/>	
The independence of the compliance function in practice	11
Moving goalposts	
Profile of compliance officers and staff	
Inadequate budgetary control	
Independence – still some way to go	
<hr/>	
The scope of compliance function activities	13
It should be more about counselling than policing	
Management still pays 'lip service'	
Optimising synergies is resource efficient	
<hr/>	
The degree of integration of compliance risk management programmes	15
<hr/>	
Overall effectiveness of the compliance function	16
Cost of Compliance: implications for remuneration	
Focus on compliance function processes	
Using technology to improve compliance function effectiveness	
<hr/>	
The way forward	18
<hr/>	
Appendix: Detailed study results	19
I. The most challenging compliance risks faced by financial institutions	
II. The independence of the compliance function in practice	
III. The scope of compliance function activities	
IV. Integrated compliance risk management programmes	
V. Overall effectiveness of the compliance function	

Foreword

Independent compliance functions will soon be a common requirement across all financial sectors in the European Union (EU). The Markets in Financial Instruments Directive (MiFID), which went live in November 2007, imposed on investment firms requirements similar to those then existing for banks. Solvency II will introduce equivalent requirements for insurance and reinsurance companies. Against this backdrop, we felt it was time to revisit our 2005 survey and assess the progress compliance functions have made in meeting the challenges facing them.

Many financial institutions, hoping for a regulatory pause following the European Commission's Financial Services Action Plan, have instead seen the number and complexity of new regulatory initiatives increase sharply. The financial crisis has led to some radical rethinking in the EU of the approach to regulation and supervision, with a general consensus, among regulators and politicians alike, that corporate governance and risk – including compliance risk – oversight need to be improved.

This report considers the results of the study against a backdrop of relevant recommendations in, for example, the de Larosière¹ report, the Turner² Review and the Commission Communication of 4 March 2009³. Among other things, these recommendations focus broadly on ensuring a principles-based approach to the establishment and operation of compliance functions while enhancing the commonality of rules across Europe. Although these aims are conceptually sound, in practice they are resulting in an environment that is anything but simple to understand – compliance heads struggling to recruit staff with real business acumen to enable them to position the function appropriately within the business. Yet, regulators are expecting compliance officers to understand and drive a compliance regime predicated on businesses being run with a compliance mindset. Our study paints a picture of a function that is increasingly expected to do more with less: both regulator and management expectations continue to grow while belts are tightened. In this context, it is essential that compliance officers come together to share their issues and experiences.

Essentially, the compliance function is a key component in the overall governance system and consequently is positioned to play a key role in helping senior management navigate new supervisory infrastructures and requirements. It can also help to mould regulatory expectations of governance and risk management practices and, potentially, more product-based regulation. In many ways, this crisis offers an unprecedented opportunity for a fresh approach for compliance functions, with the chance to establish the function once and for all as a trusted advisor to management and the business as a whole. Seizing this opportunity requires the joint effort of both management and Compliance.

This survey, which includes responses from 76 financial institutions based in 16 European countries, provides a snapshot of the progress firms have made in establishing their compliance functions. It examines ongoing and new challenges and provides a benchmark against which to assess the potential future role of the compliance function in today's changed environment.

It is structured in three sections: an executive summary providing a brief overview of the main findings of the survey; the main report, which examines our conclusions in more depth; and finally, an appendix that reviews the responses in detail, looking at examples of best practice and areas of particular concern.

Our sincere thanks go to everyone who participated in this study. Your contributions have provided valuable insights into how compliance functions are developing and some notions of a possible way forward. We also thank the various industry associations that have provided ideas and thoughts about the future. We thank in particular, PricewaterhouseCoopers' (PwC) regulatory and compliance specialists throughout Europe, who undertook a great deal of work in helping to conduct the survey and providing their own insights to support the analysis.

We hope you find our study illuminating and our insights useful.

Ullrich Hartmann

PricewaterhouseCoopers Germany
Financial Services Central Cluster Regulatory Leader

Nigel Vooght

PricewaterhouseCoopers UK
Financial Services Central Cluster Leader

November 2009

¹ Report of the High-Level Group on Financial Supervision in the EU, chaired by Jacques de Larosière, 25 February 2009.

² The Turner Review – A regulatory response to the global banking crisis, UK Financial Services Authority, March 2009.

³ Communication for the Spring European Council – Driving European recovery (COM 2009) 114 Final, 4 March 2009.

About this report

Purpose of the study

This sequel to PricewaterhouseCoopers⁴ global study *Protecting the Brand (2005)*⁵ focuses on developments in the continental European financial services sector and provides an updated view of the role of the compliance function.

This report uses the findings of our most recent study of compliance functions in financial institutions across Europe, building on the results of our previous study, to look at how much progress has been made in creating compliance functions that are able to deliver on regulatory expectations at a time when changing EU legislation sharpens the regulatory focus on governance and risk management systems, in which the compliance function plays an integral and important part.

Scope of the study

The questionnaire for our previous study was guided by the PwC Governance, Risk and compliance model (see page 14). That questionnaire was updated for the current study and asked 190 quantitative and qualitative questions focused on four key dimensions:

- Strategy and assessment
- Organisation
- Measurement and improvement
- Reporting

Study participants

Seventy-six financial institutions, located in 16 European countries, participated in the study. Seventy-three percent represented broad-based banking services, 17% investment management services and 10% insurance, although many of the respondents form part of financial conglomerates. Almost 60% are internationally active.

Compliance officers at group, business unit and entity level responded to the study, either through face-to-face interviews or by completing the questionnaire. The study results were enhanced by discussions with industry associations and regulators. We have also drawn on PwC's thought leadership literature in this field, as well as our network of regulatory and compliance specialists across Europe.

Countries represented

Austria	Germany	Luxembourg	Slovakia
Belgium	Greece	Netherlands	Spain
Czech Republic	Ireland	Poland	Sweden
Denmark	Italy	Romania	Switzerland

Conventions used

Throughout this report, heads of compliance are referred to as 'compliance officers' as opposed to 'compliance staff': we recognise, however, that this terminology may not be used in the same way in every country covered by the study. Compliance functions are referred to throughout the report either as 'compliance functions' or 'Compliance'.

⁴ 'PricewaterhouseCoopers' refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

⁵ *Protecting the brand: the evolving role of the compliance function and the challenges for the next decade*, May 2005.

Executive summary

Protecting the brand 2009

Executive summary

Introduction

Our report examines the four key dimensions of our study in the light of five main areas of interest:

- The most challenging compliance risks faced by financial institutions
- The independence of the compliance function in practice
- The scope of the compliance function's activities
- The degree of integration in compliance risk management programmes
- The overall effectiveness of the compliance function.

One conclusion is beyond doubt: none of these areas can, or should be, considered in isolation.

The most challenging compliance risks faced by financial institutions

Participants see the *'sheer and increasing complexity of the regulatory environment'* as the most challenging compliance risk for their organisations – a response that echoes the results of our previous study. In contrast with our earlier findings, however, there are now two key areas of focus:

- 1) Enhanced focus on regulatory risk management:** There is much greater recognition of the need to comply with the broad range of more demanding regulation, from the Financial Services Action Plan and more recently from the financial crisis, and also the need to manage regulatory risk in its wider context. Compliance officers increasingly appreciate the need for a coherent dialogue with regulators to gain a better understanding of their changing expectations and the need to monitor the upstream risks of new regulations more effectively.
- 2) Rebuilding customer trust:** compliance functions have an important role to play in rebuilding customer trust, which has been badly shaken by the financial crisis. Additionally, investor expectations are changing as a result of state intervention and increased public ownership, requiring these financial institutions to consider more closely the social implications of their policies. Most compliance officers do not currently see *'acting as a champion of the customer'* as one of their objectives, despite quality of service to customers being identified as a cause for concern. This will have to change.

The independence of the compliance function in practice

Considerable attention has been paid to appropriate organisational structures and reporting lines for the compliance function since our previous study and most organisations now have some form of matrix structure, designed to safeguard the function's independence. The majority of respondents report either directly to the board, or have access to it, and use standard compliance policies and procedures to facilitate a consistent compliance approach throughout the organisation.

However, significant threats to the independence of compliance functions remain through an unclear or changing mandate, inadequate resources and lack of control over their own resources.

The scope of the compliance function's activities

As a compliance function matures, its focus naturally shifts: moving from compliance policies to processes, and then towards more holistic and integrated compliance programmes. However, the responses do not necessarily suggest a constant, considered evolution.

Management still pays lip service

Organisational attitudes to compliance have improved since our previous study: for many, the compliance function's profile within the organisation has improved markedly. However, the concern that management expectations are moving well beyond existing compliance resources is a constant theme. In this respect, the maturity of the compliance culture within the organisation as a whole remains a concern. Embedding a compliance mindset, generating not just awareness but conviction throughout the organisation, is still often perceived as a responsibility of the compliance function. While compliance officers are willing and able to take a significant role in making this happen, they feel – rightly – that this responsibility remains with the board and senior management.

The degree of integration in compliance risk management programmes

Firms still have a long way to go to establish integrated compliance risk management programmes, although the majority of the respondents are moving in this direction.

In parallel with our ‘three lines of defence’ concept (see page 16), increasing attention is being paid by leading institutions to optimising synergies between different risk and control functions to complement the compliance function, identifying core competences of different functions and departments and bringing these to bear to support compliance function activities.

The overall effectiveness of the compliance function

Although resources are currently tight, regulatory expectations are cushioning the compliance function, to a certain extent, from some of the cost-reduction pressures created by the financial crisis, but it is still expected to do more with less. However, even without the cost pressures arising from the financial crisis, senior management often failed in the past to provide the appropriate tools and technologies to streamline the function’s activities and enhance its effectiveness. There has been considerable attention and investment in technologies dealing with ‘critical’ compliance requirements such as anti-money laundering rules, the breach of which has potentially significant consequences for the organisation. However, a systematic approach to embedding compliance-related controls in existing and new systems is still lacking in many firms, even though these can significantly ease the burden on the compliance function and prevent some rudimentary, but important, compliance failures. Some firms have yet to appreciate that getting Compliance involved at the user acceptance phase is just too late. There has also been very limited investment in tools designed specifically to streamline the activities of the compliance function itself.

Looking ahead, as we start to put the financial crisis behind us, and political – and perhaps regulatory – scrutiny weakens, it must only be a matter of time before senior executives (again) begin to question how, and how effectively, the compliance function enhances the quality of the business. More mature compliance functions are making progress identifying, developing and using suitable key performance indicators (KPIs) to monitor the performance of the compliance function. Quantitative and qualitative KPIs are being considered for the wide gamut of the function’s work to be used as current and future drivers for compliance function goals and objectives. However, the study shows that progress is slow and incomprehensive. This is clearly an area for future attention.

In parallel, the financial crisis has driven regulatory⁶ and political calls for firms to reappraise the remuneration system for management and all staff who impact the risk profile of the organisation (including compliance officers and staff). Clearly though, an organisation-wide assessment and appraisal system that looks beyond financial measures to encompass risk management and compliance-related considerations can greatly help to optimise the organisation’s appreciation of the risks it runs and the effectiveness (and value) of the compliance function. If senior management clearly allocates responsibility to the business to manage its own risks, the compliance function can become an important strategic management tool for ensuring that the business can continue to prosper, however complex the regulatory environment may become.

The way forward

The financial crisis will continue to have a profound impact on the financial sector across Europe and more widely. A new wave of legislation is anticipated at the EU level, in parallel with specific national initiatives to tighten existing requirements. While it may take some time for regulators to develop and adopt these new requirements (although not so long as in the past), they should influence the work of the compliance function immediately.

The changing environment will mean more – and more demanding – expectations on compliance functions from management and supervisors alike. Compliance officers must seize the opportunity to influence those expectations proactively.

Considered steps taken now to embed compliance – instilling ownership for the first line of defence effectively in the business – will, over time, safeguard the compliance function’s full value as the second line of defence, and accelerate the adoption of a compliance culture throughout the organisation.

To win back client trust in the short term means looking beyond ‘basic compliance’ to ‘integrity’. Rather than placing reliance on a constant ‘push’ from the compliance function, organisations must establish a new mindset that prevails throughout each and every part of the organisation.

An integrated approach to Governance, Risk and compliance (see page 14) increasingly reflects regulator and broader stakeholder expectations.

⁶ See for example Commission Recommendation complementing Recommendations 2004/913/EC and 2005/162/EC as regards the regime for the remuneration of directors of listed companies, C(2009)3177, 30 April 2009; Commission Recommendation on remuneration policies in the financial services sector, C(2009)3159, 30 April 2009; and Communication from the Commission accompanying Commission Recommendation complementing Recommendations 2004/913/EC and 2005/162/EC as regards the regime for the remuneration of directors of listed companies and Commission Recommendation on remuneration policies in the financial services sector, C(2009)211 Final, 30 April 2009.

Key messages

For senior management

- 'Tone at the top' is not just jargon: the drive for integrity needs to pervade all activities, internal codes of conduct and communications within the organisation
- The impact on the organisation of the changed and changing regulatory and political agenda needs to be fully understood
- Involve Compliance in rebuilding client trust
- Reach out proactively to regulators and rule makers to discuss, and demonstrate, the effectiveness of your compliance arrangements
- Consider additional measures to bolster the independence of the compliance function, in particular through:
 - appropriate organisational structures and reporting lines
 - the provision of adequate resources: human, financial and technological
 - ensuring that Compliance can draw effectively on the expertise of key support functions within the organisation, such as HR, legal and, importantly,
 - re-emphasising the advisory role of Compliance and the responsibility of business management for managing compliance risk
- Embed the 'three lines of defence' model in the organisation in order to set in stone the roles and responsibilities of the business, compliance, Risk and Internal Audit, and the relationships between them in managing compliance risk
- Engage with Compliance and ensure that compliance considerations are fully factored into the formulation of strategy and business decision-making
- Enforce the use of disciplines used in other areas of risk management in the management of compliance risk
- Monitor the performance of business management in managing compliance risk through the establishment of key compliance performance indicators
- Remember that however immaterial a subsidiary or branch may be to the group as a whole, a breach of regulations can still significantly damage the wider reputation and business of the organisation.

For compliance officers and staff

- Be proactive, and think outside the box: avoid the 'tick box' approach. The financial crisis, if anything, offers a window of opportunity to help management address trust issues with regulators and clients
- Show initiative: identify opportunities to improve the approach to the identification, assessment, management and monitoring of compliance risk in your organisation
- Focus on developing the commercial expertise of your compliance professionals: broaden their perspective by embedding an understanding of the way the business works, its products, service offerings and operational processes
- Strengthen relationships with other departments and collaborate with them: seize opportunities for synergy and benefit fully from their 'core competences'
- Continually enhance your own expertise and skills
- Don't wait to demonstrate the value that the compliance function brings to the organisation: continue to build relationships with the business so they have the opportunity to understand you and you can understand them
- Reach out to experienced compliance professionals in other organisations through industry or compliance associations to complement in-house expertise and experience.

Overall considerations

- Do not wait for new legislation: strengthen your compliance approach and organisation now
- Focus on embedding an 'integrity' mindset, rather than a 'compliance' mindset: look beyond the narrow legal parameters of compliance requirements to provide a better safeguard of your clients' interests
- Focus on the long term, but also on the means to demonstrate the results of this in the short term.

Reflections on the results of the study

Protecting the brand 2009

Reflections on the results of the study

Introduction

Considerable progress has been made by firms in developing and establishing their compliance organisations since our previous study. Firms have focused on organisational structures and reporting lines for their compliance functions, drawn up compliance risk inventories, undertaken compliance risk assessments, and put into place compliance monitoring, reporting and review processes. That said, there are substantially different levels of sophistication among firms surveyed and while some compliance functions have been operating for several years, others are newly established.

One common, ongoing challenge for all compliance functions is how to align themselves closely with the business while retaining their authority and status as an independent function. Another is to ensure that the compliance function is positioned and perceived throughout the organisation as a vital part of the firm's system of governance. This, of course, is almost impossible without the necessary focus – and action – from top-level management, of which there was limited evidence in our study.

‘The intense focus on the adequacy of the financial regulatory system will not abate any time soon. There will be no return to the status quo ante. The decisions that we take over the coming months will shape our financial markets and economies for decades. We need to make sure that our regulatory response addresses the right issues – that regulators do not try to win the last war, but that they draw the right conclusions on what is needed to police the new market structures that are already starting to emerge.’

Charlie McCreevy, European Commissioner for Internal Market and Services – Private Equity: Progress On Disclosure And Transparency (Walker Guidelines) – British Venture Capital Association London, 11 December 2008.

Firms face stricter laws and regulations, continued political intrusion and harsher demands from supervisors. From crisis comes opportunity. Now is a good time for senior management to determine the future role of the compliance function: in particular, how it can move beyond minimum regulatory requirements and bring value to the organisation as a whole. It is also a good time for the compliance function to establish itself as a key advisor that can help management successfully navigate the new regulatory landscape.

Our report examines the four key dimensions of our study in the light of five main areas of interest:

- The most challenging compliance risks faced by financial institutions
- The independence of the compliance function in practice
- The scope of the compliance function's activities
- Integrated compliance risk management programmes
- Overall effectiveness of the compliance function.

One conclusion is beyond doubt: none of these areas can or should be considered in isolation.

The most challenging compliance risks faced by financial institutions

Compliance officers participating in the study continue to see *‘the sheer and increasing complexity of regulation’* as their most significant challenge, in line with both our previous study and the Banana Skins surveys PwC produces in association with the Center for Financial Services Innovation (CSFI). The 2008 Banking Banana Skins survey showed that *‘the concerns expressed about over-regulation in earlier Banana Skins surveys remain strong: its cost and clumsiness, the growth of compliance risk, the impact on competition and innovation, the fact that those who create regulation tend to measure it by size rather than quality, the moral hazard that transfers management responsibility from bank to regulator.’* This sentiment is echoed in Insurance Banana Skins (see box).

Over half of respondents consider *‘changing regulators’* expectations a significant compliance risk. This will surely increase as new regulations continue to be rolled out following the financial crisis.

The financial crisis has resulted in increased regulatory requirements and supervisory scrutiny, both within Europe and elsewhere. Regulators are focusing much more on market integrity and interconnectedness. In Europe, the regulatory architecture,⁷ both

regionally and nationally, will change dramatically when macro-prudential requirements are introduced to complement a reinforced micro-prudential supervisory structure in line with the Commission's proposals.⁸ Systemically important market participants (including hedge funds) will find themselves subject to EU regulation and supervisory oversight for the first time. The overall approach to group supervision, both on a regional and international basis, will be upgraded with the ongoing establishment and reinforcement of colleges of supervisors for cross-border firms. So, the complexity of regulation – and the regulatory framework – will increase significantly in the short-to-medium term.

What are the implications for compliance functions? compliance officers have not shared the blame for the financial crisis with management and, to some extent, their risk management counterparts. Nonetheless, increased focus on internal governance systems will clearly have a long-term impact on their day-to-day activities, not least through increased management expectations. Two issues need highlighting: the future interaction with i) regulators and supervisors and ii) customers.

Enhanced focus on regulatory risk management

There is much greater recognition of the need to monitor upstream compliance risks and communicate regularly with regulators to gain a better understanding of their changing expectations. Similarly, changing customer and investor expectations – particularly as a result of state intervention and public ownership – are requiring compliance functions to move beyond simply ensuring compliance with specific regulatory requirements to consider the wider compliance implications of business decisions.

'The risk of too much regulation (No 5) has fallen from the top position it occupied in the last study. But it has not disappeared, only been overtaken by more urgent issues. There is now widespread concern that the crisis will trigger a regulatory crackdown on the financial sector which will put pressure on the insurance industry to increase capital and take on more compliance costs at a time when resources are very stretched. The insurance sector feels that it may be unjustly penalised for the sins of the banking sector.'

Insurance Banana Skins 2009.

Criticism of regulators' behaviour before and during the financial crisis is resulting in more challenging, intrusive, and more forward looking, supervision. Regulatory risk management will also become more challenging in the short-to-medium term as both regulators and supervisors adapt to new supervisory architectures and regulations. Firms should consider additional, proactive steps to ensure the dialogue with both their regulators and supervisors remains coherent and constructive.

There is clear evidence that more holistic approaches to managing regulatory risk have been adopted and that the majority of respondents appreciate that effective regulatory risk management goes beyond simply complying with regulations, to monitoring upstream regulatory developments and creating a coherent dialogue with regulators.

Staying on top of regulatory developments

Regulators and politicians are showing themselves to be less inclined than in the past to take industry views into account, and require thorough justification. To a greater or lesser extent, all firms need to track regulatory developments at the international, European and national levels, in order to obtain early indications of possible changes. This will permit a thorough assessment of the impacts for the organisation quickly enough to develop sufficient justification to influence the debate, if necessary. In order to influence the outcomes, contributions to the regulatory debate will need to be well reasoned and pragmatic.

According to the study results, compliance often shares responsibility for monitoring upstream regulatory risks with the legal department although, at the local level, responsibility is often passed to the business, with the compliance function providing support. In spite of firms recognising the need to monitor upcoming developments, respondents still believe their firms are mostly reactive to new regulation. The responses suggest a lack of clear management direction in terms of the assessment of evolving legislation: only 12% of respondents say that the public affairs/government relations department has a strong influence on compliance function objectives.

New or changed regulations will bring the usual compliance challenges but the timeframes for adoption are likely to be shorter than in the past. There are strong fears of a politically motivated 'knee-jerk' regulatory reaction to the financial crisis in many areas. We have already seen some evidence of this with rapid adoption of EU legislation amending the Capital Requirements Directive and regulating credit rating agencies, an unusual characteristic of which was their short implementation timeframes. With the European Parliamentary elections in June 2009 and the appointment of a new Commission later in the year, there may be a slight pause before further legislation is adopted. However, political impetus is likely to remain strong for some time and tight implementation deadlines might become much more of a feature in the future. To ensure no surprises, or last-minute scrambling and the associated unnecessary expense, particular attention should be paid to monitoring new regulatory proposals.

Changes will also occur without significant amendments to underlying legislation. Throughout Europe, there will be more convergence and consistency in both regulatory and supervisory approaches, through the work of the Level 3 committees (and their future incarnations) to create a single rulebook and through the Commission's efforts to remove unwarranted

⁸ See Commission proposals for a new supervisory infrastructure, 23 September 2009: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1347>

national options and discretions from legislation and ensure consistent legislative interpretations. However, even with such initiatives underway, national measures may still diverge upon implementation, given the volume of changes proposed and the speed with which they may be introduced. The consequences of noncompliance, however, may become more severe.

National industry associations across Europe have increased the level of assistance they provide to help their members keep abreast of new regulatory developments since our previous study. Such assistance will become increasingly important, to ensure that all firms can track changes and to enable smaller, or less risky, firms to communicate any concerns to regulators on a timely basis. Certainly, the current supervisory reform agenda is unlikely to lead to a radical rethink of risk-based supervisory approaches: the need to optimise scarce supervisory resources will remain. Smaller and less risky organisations are unlikely to receive direct regulatory attention on an ongoing basis and industry associations' importance as an information source and communication vehicle may increase. Firms need to consider whether their industry associations have sufficient resources to support them in this area.

Map changing expectations of regulators

Combining the detailed mapping of current regulatory and reporting requirements that many respondents have undertaken with an understanding of the current organisation structure and the modus operandi of key regulators (and supervisors) will enable firms to monitor organisational shifts that may impact future expectations. A number of national regulators have sought additional resources to reinforce their current regulatory and supervisory capabilities. The UK FSA, for example, announced in its 2009/10 business plan that it aimed to recruit some 280 supervisors from industry, adapting their pay scales to market rates to facilitate this. Recruiting such a large number of new staff (in this case, more than 10% of the existing workforce) in a short space of time would cause a cultural shift that would initially be most noticeable in the supervisory divisions, but would, in time, also influence policy and legislative activities.

The goalposts will continue to move as regulators get to grips with changes to their organisations and the new regulatory agenda. Assessing the impact of any changes on current strategies and operations quickly will enable firms to adjust to changing requirements in a considered way. Clearly, regulatory risk management could become much more challenging as supervisors adapt to new supervisory architectures and enhance both their skills and supervisory tools.

Reconsider who should be the primary interlocutors with regulators

The study shows respondents have diverging approaches to interfacing with regulators: some with one or a limited number of interlocutors, some with many. In some cases, regulations may predetermine the compliance function's role as the primary

interlocutor. However, this is not the norm in the countries participating in the study: regulators preferred multiple points of contact given their diverse informational needs.

A logical approach would be to align the communication strategy with the supervisory approach for each firm. Now is a good time to reassess this interaction and reconsider who within the organisation is best placed to speak to regulators on different issues, particularly in relation to new issues arising from the financial crisis. Consideration should also be given to effective internal communication of regulators' expectations by these interlocutors in order to safeguard the coherence and consistency of the interactions, particularly in terms of formal reports and responses to requests for information from the regulators. It is worth noting that the study provided no clear indications that, whatever the approach, interactions are monitored and communicated systematically within the organisation more widely. Good practice, however, suggests that Compliance should, at the very least, maintain a central record of all correspondence with the regulator.

Coherence and consistency of the interactions are likely to be especially important in a group context for organisations for which a 'college of supervisors' has been, or will be, established. The colleges should, in the longer term, rationalise supervision at the group level but they will need time to find their feet. A coherent, focused and frank dialogue will facilitate the wider appreciation of the risks inherent within the group as a whole, and to ensure that, overall, the supervisory approach is commensurate with the 'nature, scale and complexity' of the organisation – fully respecting the proportionality principle.

Firms should generally consider the possible impact of the transformation of the current Level 3 Committees to Supervisory Authorities. The overall approach to group supervision will be upgraded for cross-border firms, but, as suggested earlier, all firms will be affected by the associated push towards supervisory convergence and a single rulebook, including increased harmonisation of administrative sanctions.

Properly calibrate the role of the compliance function

Clearly, the compliance function should be a key advisor and contributor to (and participant in) the management of the relationship with regulators. Where there is no specific requirement for this, the contribution of the compliance function should be determined according to the resources it has available (compared with other potential interlocutors) and the level and nature of regulatory risk.

While it is important to note that compliance officers do need direct contact with regulators as they are best placed to understand regulatory expectations, it is also important that Compliance should not be placed as a buffer between management and regulators in terms of the relationship overall.

Rebuilding customer trust

The quality of customer service is flagged as a cause of concern in the study. Although Compliance has historically focused on adherence to specific requirements, such as Know Your Customer (KYC), consumer and data protection regulations, it is also well placed to focus on wider reputational and commercial considerations essential to rebuilding customer trust.

Information from clients

A large number of respondents are now focussing on integrating customer information: 68% have adopted, or are adopting, an integrated approach to anti-money laundering (AML) and MiFID KYC information requirements, for example. Rationalising the client acceptance procedures, creating a single collection point for all key data, and streamlining related information systems can provide a sound basis for ongoing customer relationships. Aligning these initiatives with data protection measures and record retention can significantly improve the dialogue with customers.

Information to clients

Effective communication with clients is paramount. Current EU rules focus on the need to provide customers with 'fair and not misleading' information, sufficient to enable them to take informed decisions. Recognising that different customers have heterogeneous informational needs depending on the nature of the financial services offered and the financial literacy of the customer, and, as far as possible, providing information that is 'fit for purpose' will enhance relationships and help rebuild trust. This is a theme that regulators are now revisiting.

Revisit approaches to client categorisation and associated processes

In light of the financial crisis, some regulators now believe that the granularity of client categorisation requirements (for example, in MiFID) may not be sufficient. Existing assumptions on the 'professional' nature of certain customers may need to be reassessed and attention to suitability and appropriateness assessments extended beyond pure 'retail clients'.

Further consider the product life-cycle

Regulators are likely to focus much more on product life-cycles in future. In times of boom, innovative and risky products, designed for a select group of customers, can quickly become 'mainstream' as significant rewards seem available. Future attention is likely to focus on: i) how to communicate the risks coherently to a wider, heterogeneous group of customers; ii) the timing when products can be made available to a wider clientele; and iii) altering product features to reduce risks/improve client understanding.

Focus on complaints handling

Prompt and fair complaint resolution is also fundamental for rebuilding trust. Many respondents confirm that responsibility for complaint resolution lies with the business units that deal with the client. The compliance function advises, and oversees

resolution by, the business or a complaints handling department. The study shows significant differences in the role of the compliance function with regards to the complaints handling department: some having direct or oversight responsibilities for the function, others receiving information only on request. Those differences provide some food for thought. Complaints can build to form a pattern for concern. Firms might consider adopting a similar approach to the analysis of complaints, as that adopted by some for compliance breaches.

Conflicts of interest

The study raises questions as to whether respondents (where applicable) have made sufficient progress in implementing MiFID requirements on conflicts of interest management. While a large majority have undertaken a conflicts mapping exercise, there is limited evidence of a comprehensive approach. Conflicts management is not a simple task, as the challenge is multidimensional, with constant focus on day-to-day management and long-term strategic and structural aspects. However, managing conflicts effectively – or disclosing them when this is impossible – has become more critical in the current climate.

The independence of the compliance function in practice

Are compliance functions really independent? For the majority of respondents, the answer is 'no'.

Since our previous study, considerable attention has been paid to appropriate organisation structures and reporting lines for compliance functions: different variations on a matrix structure are now evident in most organisations. The use of standard compliance policies and procedures to facilitate a consistent compliance approach throughout the organisation is also widespread.

However, the study suggests that there remain significant threats to the independence of compliance functions.

Moving goalposts

The independence of the compliance function is premised, among other things, on a clear mandate. Compliance officers are generally involved in setting and agreeing their functions' objectives with the board and senior management, with 83% seeing the board of directors as most influential in this regard. However, goals and objectives are not always clear and a wide-ranging remit is often combined with changing management expectations. Respondents worry that the goalposts are constantly moving (for example, towards advising on prudential issues and sustainable value creation, and more broadly on reputational risk management), without an associated reassessment and/or reallocation of resources.

This not only sets a foundation for inefficiency but also creates an environment where the purpose, validity and value of compliance function activities and advice can be called into question. In many cases, respondents feel the goalposts are moving. This is an increasing concern as firms strive to respond to increased regulatory, political and public expectations.

To be effective, the compliance function should have a clearly defined mandate that establishes its role within overall governance structures of the organisation, reflecting a pragmatic and generally more granular approach to managing regulatory and reputation risk. This means that, in relation to specific regulatory and reputation risks, its role and objectives need to be carefully calibrated with those of other functions, such as the legal department, internal control, risk management and internal audit, optimising synergies wherever possible. The calibration should reflect the extent to which a compliance culture is embedded within the organisation, but also be gauged to promote ongoing efforts in this area. This challenge is unique to every firm.

An appropriate compliance structure needs to be established, together with a clear mandate, against the backdrop of senior and business management's sustained promotion of a compliance culture and continuous emphasis on the important role played by the compliance function. Responsibility for communicating compliance function objectives however is often delegated by management to the compliance function itself. However, as one respondent notes, ideally the compliance function's remit should not only be approved by the board, but also communicated by management as part of an ongoing communication exercise designed to encourage compliant behaviours within the organisation.

Profile of compliance officers and staff

The compliance function also needs to remain close to the business. The danger is that a close relationship with the business and reporting regularly to local management might jeopardise Compliance's independence and ability to influence. However, the ability to influence both depends on and reinforces the compliance function's credibility.

Although most compliance officers participating in the study are sufficiently senior to enable them, in theory, to influence business line management with authority and still safeguard their independence, our study suggests that, for many, this is still an ongoing dilemma. Compliance officers note that their ability to influence depends not just on seniority but also on their capacity to relate to the commercial mindset of the business and understand the nature of the business. These challenges are exacerbated when it comes to more junior compliance staff.

Some firms are addressing this issue by importing staff with broad commercial awareness and deep, relevant knowledge of key products, business lines or risks into the function from the business or other control functions. Ensuring that compliance

officers and staff have, or have access to, appropriate expertise can increase their effectiveness. Specific attention needs to be paid to appropriate training and development programmes for compliance officers and staff, particularly when they grow within the compliance function. Centres of expertise within the (group) compliance function can also be used to support compliance officers and staff in branches or subsidiaries who have insufficient resources to cover all the (new) broad-ranging business issues handled in the branch in depth.

Given the broad range of responsibilities of compliance functions, the composition of the function itself needs careful consideration, ensuring that Compliance encompasses a diverse range of skills. There is a growing need for specialists in the compliance function. Increasing regulatory demands are making it ever-more difficult for small compliance teams to develop and maintain a deep knowledge of compliance requirements and a broad awareness of the commercial aspects across all products and business lines. However, the overall management of the compliance function also needs attention. Larger compliance functions should focus on ongoing enhancement of compliance officers' management skills. In larger organisations that require a broad range of specialisms, there is a crucial need for sound managerial, team- and relationship-building capabilities. Compliance officers also need highly developed influencing skills to manage such a diverse set of individuals and the differing expectations of internal shareholders, without jeopardising the function's independence.

The credibility of compliance officers can be reinforced externally. Current proposals for Solvency II indicate that 'fit and proper' assessments will apply to compliance officers and this may well extend in time to other financial sectors as well as insurance. As a related issue, it is important to note that personal liability of compliance officers, which exists in a number of countries, can have negative consequences particularly if the compliance officer is not sufficiently influential within his or her organisation.

Industry associations are proving increasingly valuable in helping organisations stay abreast of regulatory developments. However, they do not necessarily cater for the specific needs of compliance officers. Only a few countries, such as the Netherlands, have followed Luxembourg's lead in establishing an association specifically for compliance officers, although some have set up compliance-focused units within sectoral or cross-sector industry associations (such as Febelfin in Belgium). In 2005, one regulator suggested that the establishment of a national (and international) compliance officer association could not only provide a good interlocutor for regulators, but also that such associations would enhance the 'professionalisation' of the compliance officer role, inter alia through training and development initiatives. Given the findings of this report, we would recommend that this suggestion receives more consideration.

Inadequate budgetary control

Fifty-two percent of respondents indicate that they do not have full discretion over the financial resources allocated to them. Most respondents' compliance budgets are subject to negotiation and then board approval. However, 64% of respondents indicate that they subsequently have either partial or no control over their approved budgets. Furthermore, the approved budgets often focus on direct salary and associated costs, rather than broader operational considerations. This impacts the compliance function's independence in a very practical sense: can the compliance function, for example, influence the organisation's compliance agenda appropriately and subsequently allocate suitable resources to carry it out? It may also reduce the speed with which new compliance risks can be addressed.

Independence – still some way to go

Other study findings show limited compliance involvement in strategic decision-making and worries over internally generated compliance risks, which reinforce an overall impression that the compliance function is not strong enough in some organisations to perform its role effectively. Incomplete or poorly implemented compliance risk management plans, inadequate breach escalation processes and, in some cases, the relative infrequency of reporting to management or the board, add weight to this statement.

On a positive note, however, it appears that significant attention has been paid to reporting. A large majority (78%) have formally documented the compliance function's reporting lines and communicated these throughout the organisation. Board involvement is relatively high across most respondents: all respondents report to the board of directors (i.e. to the full board or a specified committee) – 75% directly and 25% via senior management. Forty-five percent submit quarterly or more frequent reports to the board, and 51% report to senior management on a quarterly or more frequent basis.

The scope of compliance function activities

The list of compliance function activities used in the questionnaire for our study was originally derived from circulars issued by the Belgian financial regulator⁹ (see box opposite).

Our study findings show that this range of activities for compliance functions is now widely accepted throughout continental Europe. Although, on aggregate, the statistics for time spent on the various activities is comparable, there are notable differences when looking at individual responses (see page 39).

It should be more about counselling than policing

Organisational attitudes to compliance and the compliance function have improved since our previous study; for many, the compliance function's profile within the organisation has improved markedly. A number of respondents specifically note that MiFID has enhanced the compliance function's profile in general within their organisation.

The differences our study reveals in the perceived role of management in terms of the compliance risk management programme however begs the question – Is management always clear on its fundamental responsibility for organisational compliance and what this means in practice?

In our previous study, we discussed finding the balance between the 'police officer' and 'counsellor' roles of the compliance function. For many respondents, that equilibrium has not yet been reached. Some respondents feel the pendulum had swung too far in the direction of 'police officer', sometimes as a result of specific regulation, such as MiFID or AML.

Compliance function activities

- To help the organisation anticipate and plan for changes in regulations
- To ensure that reputational risk is being managed effectively
- To ensure that the organisation is compliant with regulations
- To act as a champion of the customer within the firm
- To influence the regulatory agenda/processes in the interests of the firm
- To ensure that regulatory risk is being managed effectively
- To ensure compliance with regulations, as well as internal and external codes of conduct, in the development of new products and markets
- To train and educate staff in regulatory requirements and the requirements of internal policies and procedures
- To build greater confidence in the organisation on the part of the client
- To act as a central repository of all information on rules, codes and business practices, and ensure dissemination to all appropriate people within the organisation
- To advise business units on how to ensure that (new) services and products are, and remain, compliant
- To advise senior management on managing compliance risk
- To provide assurance to the board of directors that compliance is being adequately managed.

⁹ See Circular D1 2001/13 to credit institutions, 18 December 2001; Circular D1/EB/2002/6 to investment firms on internal control as well as the internal audit and compliance functions, 14 November 2002; Circular PPB/D.255 to insurance companies, 10 March 2005.

However, many respondents stress that it is not actually a question of balance: they believe Compliance's primary role should be to advise management and the business on how to remain compliant. Many responses though suggest that the compliance function faces difficulties in ensuring that its responsibilities are properly calibrated.

Management still plays 'lip service'

'Tone at the top' means the board and senior management set the tone for compliance standards that the whole organisation lives by. This is an ongoing, constant process that should permeate every area of management, business and the control environment. A different emphasis in terms of the activity of the compliance function, as evidenced by the shift in focus noted above may reflect improving maturity of the compliance culture. However, this appears to have happened almost unconsciously: the responses do not suggest a continuous, planned evolution.

The responses indicate that, while management does not necessarily see the compliance function as a control function, compliance's advisory role is still sometimes contested and its involvement in broad strategic considerations is often limited. Management's perception in terms of Compliance's contribution to achieving strategic objectives often remains hazy. For example, 64% of respondents indicate that Compliance is involved in the new product approval process, but the nature of this involvement ranges from the right to veto projects, to providing recommendations and opinions, to simply reviewing and signing-off relevant documentation.

Compliance officers are rarely asked to provide input into strategic or business decision-making in connection with wider business development and growth, such as new lines of business or new markets, or proposed mergers and acquisitions. Adapting the compliance framework to organisational changes caused by rapid expansion or growth in activities, nationally or internationally, is a significant compliance challenge, particularly after the fact. This suggests that compliance is often still an afterthought, and that management continues to pay 'lip service' to the concept.

Optimising synergies is resource efficient

This perception was supported further by the widespread contention among respondents that the compliance function within their organisation is deemed responsible for compliance with regulations – rather than responsible for assisting management and the business to become, and remain, compliant.

The study suggests that firms need to do more to 'operationalise' compliance throughout the organisation, drilling down responsibility, with the compliance function to provide guidance and help with this process. The composite list of other functions and departments that have a role to play in the compliance management programme is relatively broad, but there are substantial differences from firm to firm. All functions and departments should be required to facilitate and support the

process and the compliance function should be able to draw on 'competence centres' within the organisation, such as legal and human resources (HR), for specific expertise or support.

HR, for example, knows how to deal with people, how to get messages across, how to stimulate certain required behaviours and how to discipline people when things go wrong. The legal department, meanwhile, knows how to provide considered counsel and advice in respect of all areas of the business and also knows how to assess new legislative proposals and, where necessary, to influence them.

Optimising synergies between different functions is resource efficient. However, there are no standard recipes: each organisation needs to calibrate the tasks performed by the compliance function in line with its own resources and the support available from other functions.

The PricewaterhouseCoopers' Governance, Risk and compliance (GRC) approach and operating model are founded on three core principles:

1. Integrity-Driven Performance¹⁰ requires that organisations integrate their approach to GRC. Such an approach is critical as effective integration fosters a culture of business integrity and accountability.
2. An integrated model should link to shareholder value and effectively coordinate an organisation's people, process and technology capabilities so that Integrity-Driven Performance is embedded in the fabric of the organisation acting to support the achievement of strategic objectives.
3. Integrity-Driven Performance requires a new vision of business conduct and compliance – one that understands stakeholders' needs and supports compliance with both the letter and spirit of relevant obligations. This includes compliance with internal policies and procedures as well as managing expectations of stakeholders such as regulators, customers, business partners, employees, investors and society as a whole.

To attain a level of Integrity-Driven Performance, we believe that organisations need to get four fundamental enablers right:

1. Address and effectively manage the change to a culture of business integrity and ethical values
2. Embed an integrated GRC approach into core business processes
3. Deploy the capability to measure performance and calculate value through the right metrics and dashboards
4. Leverage technology to enable effectiveness and efficiency.

The degree of integration of compliance risk management programmes

An integrated approach to compliance risk management encompasses risk identification, assessment, monitoring, mitigation and regular reporting. Clearly, the compliance function's role in each of these areas needs to be properly established, with clear responsibilities retained by management and the business. However, all the activities of the compliance function are facets of the overall (compliance) risk management programme and, therefore, its interaction with other risk management and control functions also needs attention.

'Companies with an appropriate and measured appetite for risk – i.e. those that can see beyond the risk to the opportunities they present – are much more likely to prosper.'

Being smart about the risks you take: Get up to speed, PricewaterhouseCoopers, November 2008.

Firms are still in the early stages of establishing comprehensive compliance risk management programmes, although the majority of the respondents are moving in this direction. Sixty-three percent say they have developed and fully documented an annual compliance management plan/programme but such plans are generally a recent development. Only forty-one percent say that their programme focuses on enhancing compliance risk management throughout the organisation (rather than purely compliance function activities) and only firms with longer-established compliance functions show clear evidence of a more comprehensive, forward-looking or multi-year compliance risk management programme. Some of these firms are looking to apply more advanced risk management disciplines: 25%, for example, have made progress in identifying critical success factors for the compliance risk management programme overall. However, interestingly, forty-eight percent of respondents say the difference between the compliance management and the compliance monitoring programmes is still not fully understood within their organisation.

That said, a considerable amount of progress has been made in improving compliance risk assessment processes and associated compliance monitoring and reporting. There is a clear trend towards a risk-based approach to compliance risk management generally, however only forty-seven percent say that a risk-based approach is currently used for compliance risk assessment.

Thirty-one percent indicate that consideration is being given to determining a 'risk tolerance' in respect to compliance risk, in line with best practice in other risk areas, however the thinking in this regard is not well advanced. Many respondents to our

2005 study said management had established a 'zero tolerance' policy in terms of non-compliance with regulations and, as we have already seen, the current focus is still primarily on compliance with regulations rather than broader reputational risk issues so this result is not surprising. Where a risk tolerance has been considered, this, most frequently, is based on a relatively static compliance risk assessment, as opposed to a dynamic retuning process designed to adapt rapidly to changes in stakeholder expectations or business strategies. There is also limited evidence that compliance risk tolerance is determined according to the degree to which a compliance culture was embedded within the organisation.

In terms of the wider compliance management programme, the compliance functions can draw on expertise within other risk management and governance competence centres within the organisation to optimise their performance. Many opportunities exist for synergies with the risk management, internal control and internal audit functions that can complement resources in the compliance function.

For over half of respondents, complementary working practices exist with the risk management (fifty-four percent) and internal audit (fifty-five percent) functions. The study reveals some key areas where synergies are being to be considered and exploited by some respondents:

- The risk management function is well versed in identifying, measuring, monitoring and reporting risks: collaboration in terms of compliance risk assessments (and using risk-based approaches) is becoming more frequent
- Internal control has experience in developing and implementing controls that are practical and cost-effective; as one respondent noted, this is the 'go to' function for help on setting up appropriate risk mitigants.
- Internal audit uses well-established auditing methodologies for reviewing, sampling and testing, which can provide ideas on effective compliance oversight.

We would argue though that it is not simply a question of other functions supporting the compliance function (or vice versa as with some respondents). The mandate of the compliance function should be calibrated with the mandates of other functions, in the context of a 'three lines of defence' approach (see box). This concept, which clarifies the responsibilities of the different actors, has considerably matured since our previous study. Forty-three percent of respondents say they apply this concept to some extent, although most often in respect of AML requirements.

Effective implementation of this concept puts the compliance function squarely in the 'advisory' category (i.e. in the second line of defence). This means 'operationalising' the first line of defence where compliance control and day-to-day monitoring becomes more clearly the responsibility of the business, with the compliance function providing oversight and advice.

In practice, however, the three lines of defence can and often do overlap, depending on the organisational compliance structure (for example, with regards to 'embedded' compliance staff in the business who undertake real-time surveillance of transactions to ensure compliance with anti-money laundering, market abuse or client order handling rules, and global 'above-the-wall' monitoring of transactions). Apparent conflicts can be resolved if emphasis is placed on a clear differentiation between first-line and second-line monitoring and oversight responsibilities – assigning these to the business in the first line and the compliance function in the second (see diagram below).

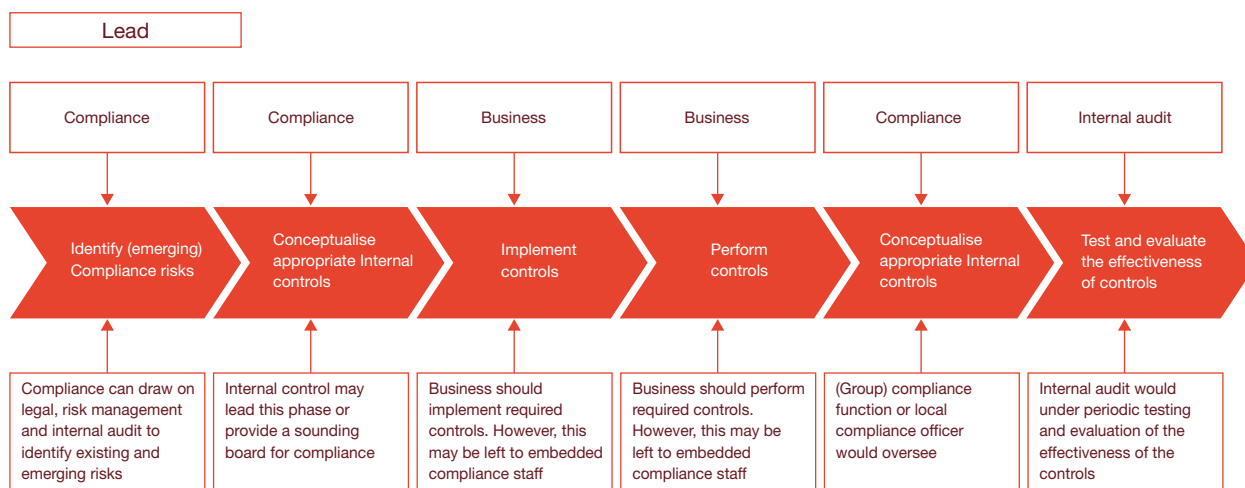
Study respondents noted that implementing the three lines of defence exposes a continuing need to reinforce the organisational compliance culture. Organisations can move progressively towards establishing the three lines of defence, systematically establishing a clearer delineation of responsibilities between the various functions over time.

Although our study shows that firms have made progress in rationalising the responsibilities of the different functions and to leverage synergies between them, there is still some way to go. While forty-five percent of respondents say other functions, such as risk management, internal control or internal audit, have day-to-day compliance responsibilities, forty-seven percent say this is the sole responsibility of Compliance, suggesting that a 'silo mentality' still persists in many organisations.

Overall effectiveness of the compliance function

Compliance officers who believe that their function's intrinsic value is self-evident may have their heads in the sand. Respondents say that management increasingly sees compliance as a means to enhance the quality of the business but, in time, it is inevitable that

The three lines of defence in practice



Source: PricewaterhouseCoopers

The three lines of defence for compliance risk management

First line: this includes people employed by the business, as well as related administrative functions. Business and operational staff have to adhere to pre-established compliance policies and requirements and perform specific controls on an ongoing basis. Administrative staff monitor associated administrative processes and perform critical controls on them.

Second line: the compliance function ensures that thorough compliance risk assessments are undertaken by the business, and monitors whether such assessments remain valid on a continuous basis. It advises the business on appropriate mitigation processes to manage the more material risks, and oversees the effective implementation of these processes. It helps management establish effective breach identification and escalation processes and ensures

their ongoing efficiency. It provides ongoing advice to the business on how to remain compliant, particularly in terms of new business (clients, products, markets) and to management in relation to proposed strategic redirections.

The compliance function does undertake specific, limited monitoring activities, where such real-time monitoring needs to be disassociated from management and business operations. This would include high risk areas, such as personal account dealing and adherence to established Chinese wall arrangements.

Third line: this aims to ensure that the overall control framework of the organisation is adequate. The first and second lines of defence are subject to functional and operational audits; compliance controls are tested as part of operational audits. In addition, internal audit request, or may be asked to perform, specific audits of compliance or compliance-related matters.

management begins to ask itself how the compliance function does this. (Given the current economic climate, this is likely to happen sooner rather than later.) The need to demonstrate the value of the compliance function will become more acute in the future.

Demonstrating this value will rely on demonstrating effectiveness. The more mature compliance functions represented in the study are making some progress in developing their approaches to compliance function effectiveness assessments, including the use of various quantitative key performance indicators (KPIs). More work is needed, though, to identify KPIs for the activities of the entire compliance function that fully reflect the qualitative (as well as quantitative) aspects of its work, and to use these as future drivers for compliance function goals and objectives. The latter should measure progress in embedding a compliance culture, as well as compliance-specific objectives, in the organisation as a whole. Sixty-three percent of respondents indicate that they have objectives for the compliance team as a whole or that they are working towards this.

While progress has been made, some of the bases for assessing the effectiveness of the compliance function are often still incomplete:

- Work is still required in many organisations to translate compliance function objectives into personal objectives for individual compliance officers and staff.
- More focus is needed on improving the processes of the compliance function itself, in addition to simply ensuring compliance with regulations.
- The use of technology to improve the effectiveness of the compliance function needs to advance.

As noted earlier, the study also shows that work is still needed to embed a compliance culture in many organisations and to ensure that the business is fully aware of its responsibilities. The introduction of individual compliance objectives as part of the performance objectives throughout the organisation is one means to 'operationalise' this awareness, crystallising responsibility between business and the compliance function.

Cost of compliance: implications for remuneration

The breadth of compliance function activity necessitates a broad skills base. Many of the compliance functions considered in the study are characterised by multidisciplinary teams, often with specialist units in certain key areas (such as AML) requiring specific skills. These are positive developments overall, but the lack of appropriate performance measures suggests that the differences in compliance staff profile, activity and performance are not necessarily adequately recognised and compensated. Significant questions remain around the development, retention and remuneration of compliance officers and staff that cost containment or reduction measures driven by the crisis may exacerbate.

This would seem therefore to be a good time to reconsider how compliance officers and staff are compensated within the wider

context of the organisation as a whole. The April 2009 Recommendation of the European Commission on remuneration in the financial sector (see box) suggests that remuneration policies for staff whose work affects the risk profile of the organisation (Compliance falls into this category) should take into consideration factors other than financial performance, and also advises against disproportionate performance-related components to remuneration packages.

'In order for remuneration policy to be in line with the objectives, the business strategy, the values and the long-term interests of the financial institution, other factors, apart from financial performance, should be considered, such as compliance with systems and controls of the financial institution, as well as compliance with the standards governing the relationship with clients and investors.'

European Commission Recommendation on remuneration policies in the financial services sector, April 2009.

In recent years, many firms have based compliance officer and staff bonuses on the performance of the organisation as a whole, rather than individual business lines or units, in order to protect their independence. However, this does not necessarily result in clear performance measurement parameters being set for either the compliance function or its members. In many ways, compliance function remuneration may still be premised largely on a 'non-event' (i.e. the absence of compliance breaches), rather than the contribution overall to guiding the organisation towards compliance. Some more fundamental thinking is therefore required around how best to reward compliance function staff going forward.

A review of remuneration structures in general offers an opportunity to think more comprehensively about the best way to assess and compensate compliance officers and staff. However, linking compensation to compliance-related performance measures for the organisation as a whole as discussed earlier may accelerate improvement in the compliance culture overall.

Using technology to improve compliance function effectiveness

While there is increased, if reactive, management attention on processes to ensure compliance with (new) regulations, limited attention is paid to ongoing enhancement of compliance function processes themselves. A lack of focus on improving compliance function processes is relatively systematic. Only thirty-three percent of respondents have developed a plan to assess and improve selected compliance processes (with only twenty-six percent reviewing such plans on an annual basis). In the majority of cases, the compliance function falls within the scope of internal audit review and its effectiveness is assessed as part of this periodic review.

This lack of focus, coupled with incomprehensive compliance risk management programmes and the concerns voiced repeatedly by respondents in relation to the 'moving goal posts' (both mentioned earlier), indicates that there are still significant challenges ahead for compliance in terms of establishing appropriate tools to ensure its effectiveness.

One way to address these challenges can be through the appropriate use of technology.

There is an increasing focus on the use of technology for compliance purposes within the organisations surveyed. However, the most prevalent use of specific compliance systems and software to date however is for monitoring purposes, with AML monitoring still at the top of the list. MiFID though has created an upsurge in the use of technology for monitoring compliance with, for example, KYC requirements more broadly, and with requirements relating to personal transactions and associated insider trading. Market evidence also indicates that more firms are adopting smart-order routing systems to help comply with MiFID best execution requirements.

Our study indicates that there is wide acceptance of the need for the compliance function and the IT security department to work very closely together (this is a considerable development from the 2005 study). There are also clear indications that synergies between these two departments are being exploited to a greater extent than they were when our previous study was conducted. However, where IT has been outsourced, the fact that the compliance function cannot draw on such support on an ongoing basis needs to be factored into its resourcing considerations.

For all these advances, in terms of its own processes, the compliance function often needs to rely on email and shared drives. Further consideration should be given to the wider use of technology to facilitate embedding compliance within the organisation and making the work of the compliance function more efficient.

The way forward

Throughout our study, participants expressed concerns that the scope of their mandate is extending far more quickly than the resources they have available. They fear – rightly – that this will, sooner or later, have negative consequences for the function's effectiveness.

To mitigate against this, management should:

- Revisit the resource issue to ensure that the compliance function's responsibilities are commensurate with the resources at its disposal (both in terms of numbers and skills).
- Review the performance of the compliance function against an assessment of how far organisation-wide compliance objectives have been established. Business management should be assessed on the degree to which it manages compliance risk, covering regulatory and reputation risk, in line with the predetermined risk tolerance.
- Focus the compliance risk management programme on processes designed to support the effectiveness of the compliance function itself, rather than just compliance with regulations. Management should also consider wider use of technology to facilitate embedding compliance within the organisation and the work of the compliance function.

In parallel, compliance officers and staff need to consider how best to demonstrate the effectiveness of the function. Its performance will increasingly be assessed in terms of value for money, and return on investment.

Appendix: Detailed study results

Protecting the brand 2009

Figure 1
 Achieving compliance



Figure 2
Sustaining compliance



Source: PricewaterhouseCoopers

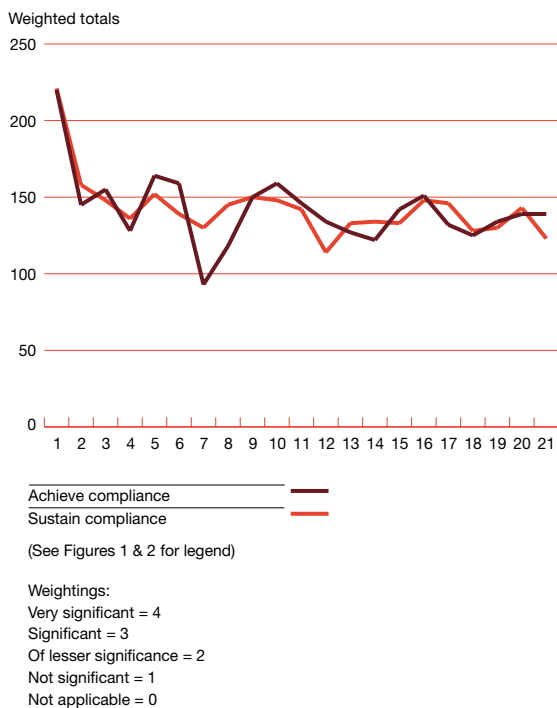
The most challenging compliance risks faced by financial institutions

Different challenges in achieving versus sustaining compliance

Respondents to our study were asked to identify which compliance risks they find most challenging. A total of 21 potential risks were identified (see legend to Figures 2 and 3) and respondents were asked to rank these according to their significance. The results show differences in the significance of the perceived challenges when aiming to achieve compliance in a particular area versus subsequently sustaining compliance.

Reflecting the results of our previous study, the 'sheer and increasing complexity of the regulatory environment' remains the most significant challenge by a considerable margin, receiving respondents' highest ranking overall, both in terms of achieving and sustaining compliance. In terms of achieving compliance, 76% of respondents see this as either a 'very significant' (51%) or a 'significant' (25%) challenge. Seventy-five percent also see it as at least a significant challenge to sustaining compliance, although those considering it a 'very significant' challenge slipped to 45%. This suggests that the sheer and increasing complexity of the regulatory environment is perceived as marginally less of a challenge once the compliance function becomes established.

Figure 3
What are the major challenges to achieving compliance?
Are the challenges different when sustaining compliance?



Other challenges score relatively highly on both dimensions. Forty-one percent of respondents rank 'changing expectations of external stakeholders' and 'an insufficient pool of talent for resourcing the compliance function' as at least significant challenges to both achieving and sustaining compliance.

In most cases, however, the challenges are rated marginally more highly in terms of achieving compliance (see Figure 3). Forty-six percent rate 'non-involvement in strategic or tactical decision making', and the 'lack of an efficient organisational structure and unclear roles and responsibilities' as either 'very significant' or 'significant' in terms of achieving compliance, while 41% and 38%, respectively, rate these as 'very significant' or 'significant' in relation to sustaining compliance.

Forty-five percent consider an 'inadequate technological infrastructure for business compliance' as at least a significant challenge in achieving compliance, decreasing to 37% in terms of those who believe this is at least a significant challenge in sustaining compliance. 'Poor coherence/collaboration between the compliance function and other risk and control functions' and 'differences in awareness/understanding of compliance issues in different national jurisdictions' are also rated more significant in terms of achieving compliance. This suggests that such challenges are also perceived to diminish as the compliance function matures.

Some challenges, however, increase over time, reflecting perhaps the dynamics of organisations as they develop. Forty percent of respondents deem 'changing expectations of internal stakeholders' as at least a significant challenge in achieving compliance, but 45% see this as a very significant or significant challenge in sustaining compliance.

Asked what other challenges they faced, respondents highlight issues that are, in the main, internal in nature:

- Achieving and maintaining the proper balance and trust with the business – in terms of providing advice and partnering the business, as opposed to controlling
- Adapting the compliance framework to organisational changes caused by rapid expansion or growth of activities, nationally and/or internationally
- The increasingly competitive environment
- Embedding a compliance mindset, generating not just awareness, but conviction throughout the organisation
- Overly high expectations, or lack of clarity, around the scope of the compliance function's remit

- Correctly calibrating the high-level governance and control framework in terms of the responsibilities of risk management, internal control and internal audit with the compliance function’s responsibilities, particularly given limited resources
- Lack of business experience and limited knowledge of complex products within the compliance function
- The ability of the compliance function to collaborate effectively with other functions in order to broaden their perspective and provide pragmatic business solutions and/or relevant alternatives
- Effective collaboration with the IT department to ensure that technology that supports the business also promotes compliance.

Sheer and increasing complexity of the regulatory environment

In considering the complexity of the regulatory environment, there are a number of issues to take into account, including current legislation that is particularly demanding; anticipated, substantial changes to legislation; and regulators’ expectations changing or increasing over time.

Existing rules are demanding

Respondents generally see existing EU legislation as demanding (see Figure 4). Not surprisingly, the highest-ranked compliance risks are:

- Anti-money laundering and combating terrorist financing (AML)
- Know-your-customer (KYC) rules
- Secrecy and privacy
- Conflicts of interest management.

AML

In line with the 2005 study, respondents continue to see rules on anti-money laundering (AML) and combating terrorist financing as the highest compliance risk overall. Seventy-nine percent see this as at least a significant risk, with 67% considering it the ‘most significant’ or a ‘very significant’ risk. Reflecting its importance, 67% of respondents retain dedicated AML compliance officers working in parallel with, or as part, of the compliance function. The most frequent use of technology by compliance functions also relates to AML (suspicious transactions) compliance monitoring and reporting.

KYC and secrecy and privacy

Seventy-two percent rank both KYC and secrecy and privacy rules as at least significant risks: ‘very significant’ or ‘most significant’ by 57% and 61%, respectively. In terms of the KYC rules, MiFID has extended the pre-existing rules for investment firms and banks. As well as the need for KYC in AML

Figure 4
What are your main compliance risks?



Weighting:
 Most significant = 5
 Very significant = 4
 Significant = 3
 Less significant = 2
 Not significant = 1
 No response = 0
 [5% did not respond]

Source: PricewaterhouseCoopers

compliance, the rules now also require specific information on a customer’s investment profile in order to ensure that, when recommending financial instruments, these are suitable and/or appropriate to a customer’s investment objectives and attitude to risk. These requirements dovetail, to a certain extent, with rules in the Insurance Mediation Directive (IMD) and national rules on ‘treating customers fairly’.

‘A fragmented approach to privacy compliance has become inadequate and outdated, let alone inefficient. Instead, firms must address customer demand, competitive pressure, and stringent, ever-changing regulatory requirements with a comprehensive, integrated privacy and data protection program’.

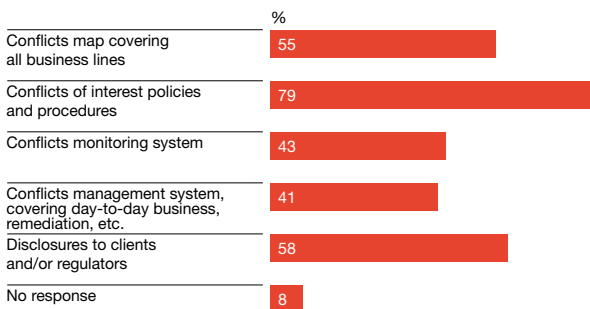
PwC Financial Services Research Institute, *The Privacy Paradox: the challenges of locking own data in an open world*, November 2008.

Sixty-eight percent of respondents say they have recently deployed, or are in the process of deploying, an integrated KYC approach covering both AML and MiFID requirements in order to rationalise and streamline information obtained from customers and the associated information systems. Some projects factor in consumer and/or investor protection, data protection and record retention requirements, requiring close collaboration between the compliance function and information security. While the majority of respondents indicate that KYC processes are handled by individual business lines, some are adopting a 'global' approach, pulling together client information across the group as a whole.

Conflicts of interest

Sixty-eight percent rank conflicts of interest rules¹¹ as, at least, significant risks (55% 'very' or 'most' significant). Progress in terms of conflicts of interest management was patchy, however. Seventy-nine percent of respondents have conflicts of interest policies and procedures in place (see Figure 5), compared with 58% who have addressed disclosure issues. Looking at a more comprehensive approach to conflicts management, 55% have undertaken comprehensive mapping exercises across lines of business, while less than half (43%) have set up conflicts monitoring systems or overall conflicts management systems (41%). A few respondents have adopted the Anglo-Saxon model of establishing 'control rooms' that are used as a tool to help manage conflicts at the global level. International respondents see conflicts management as a dynamic process, subject to constant revision and improvement.

Figure 5
Have you adopted a comprehensive approach to conflicts of interest prevention and management?



Source: PricewaterhouseCoopers

Other customer-related risks still rank highly

In addition to KYC rules, over 60% of respondents rank other customer-related requirements as at least significant, in particular: treating customers fairly (66%); customer disclosure rules (63%); and consumer protection rules (61%). Complaints-handling rules, on the other hand, are seen as significant by only 50% of respondents.

Other risks ranked by 50% or more of respondents as significant are: requirements for reporting compliance breaches to regulators; best execution and client order handling rules; insider trading and market manipulation rules; and anti-fraud legislation.

Some specific organisational risks need particular attention

There are specific organisational issues on which management is increasingly focusing. In some cases, this is clearly a reaction to recent market events. Respondents considered outsource service providers (45%), joint ventures (25%) and independent or tied agents (37%) as significant compliance risks (see Figure 6). These concerns were not, of course, relevant to all respondents.

Figure 6
What are your organisation's main non-compliance risks?



Weighting:
Most significant = 5
Very significant = 4
Significant = 3
Less significant = 2
Not significant = 1
No response = 0
[12% did not respond]

Source: PricewaterhouseCoopers

In addition, 47% see rogue employees as at least a significant risk. Overall, 50% rank 'internal organisation issues' and 45% 'technology failures in respect of technology on which compliance (monitoring) relies' as significant compliance risks.

Looking ahead, 64% of respondents consider that governance issues are likely to present the most significant challenges for the future. Twenty-five percent see globalisation as a very significant challenge, while 53% see complex structured products as the most significant or a very significant risk.

¹¹ MiFID requires an holistic approach to conflicts of interest management, including disclosure to clients where conflicts cannot be adequately managed. MiFID requirements, however, are not relevant for all respondents to the study.

Managing upstream regulatory risk: new rules and new expectations

Emerging or evolving rules and regulations

New regulation or changing expectations of regulators can create upstream regulatory risks. For the majority of respondents, the legal department, supported by the compliance function, monitors these risks. Some respondents say they consciously split the focus between upstream regulatory risks and market risks, the latter being the responsibility of business. Others put the onus on the business to monitor upstream regulatory developments at the local level, supported by the compliance function or by the legal department or, in some cases, internal audit.

A limited number of respondents have a special unit, either in the (group) compliance function or working in parallel with that function, with the prime responsibility for monitoring upstream regulatory risks. Some use outside consultants and lawyers to support these efforts.

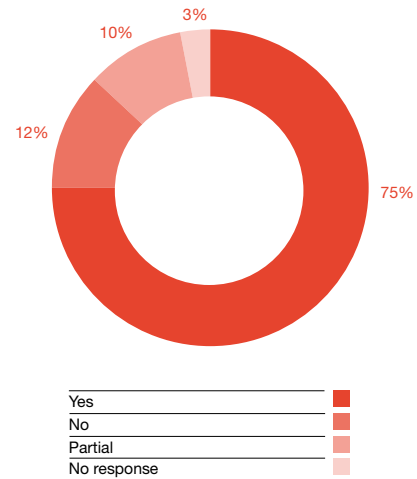
Most respondents stress the growing importance of industry associations in developing awareness and understanding of possible regulatory changes. Clearly, industry associations are perceived to be stepping up to the plate as key interlocutors with regulators. However, influencing the legislative agenda (rather than tracking the regulatory one) appears less important: public relations/government affairs departments are not seen as key internal stakeholders (see page 32).

Changing expectations of regulators

In recent years, regulators' expectations have changed as a result of ongoing cooperation, information exchange and dialogues between regulators at an international level and in Europe. These expectations have also shifted due to the changing regulator organisational structures and operating methods, or the resources available to regulators. The European drive towards supervisory convergence has encouraged constant movement. While 58% of respondents see shifting regulatory expectations as, at least, a significant risk for their organisation, only 33% see supervisory convergence as the most significant or a very significant future challenge. Recent developments, particularly the de Larosière report and subsequent reactions by the European Commission that indicate the adoption of a new supervisory structure in the EU by the end of 2010 suggest that this percentage will rise over the coming months.

Respondents believe that a direct and ongoing contact with regulators permits a clearer understanding of regulators' expectations. The majority of respondents (74%) have direct contact with regulators at the group and/or entity level in relation to the areas for which they are responsible (see Figure 7). A few respondents have formalised this interaction

Figure 7
Does the compliance function interface directly with regulators at the group and/or entity level?



Source: PricewaterhouseCoopers

in their annual compliance management plan. One respondent has a specialist unit within the compliance function responsible for all communications with the regulators. In a few cases, however, the interaction is either extremely limited (for example, submission of an annual report) or nonexistent.

The compliance officer is sometimes an organisation's sole point of contact with the regulators. For many, however, there are multiple contact points at both the group and entity level, reflecting the diverse information needs of the regulators. Other interlocutors include management, the legal department, risk management, finance and internal audit. Generally, restrictions are applied, with only nominated individuals permitted to interact with the regulators. However, concerns are still expressed that multiple contact points can be detrimental to the coherence of these communications. Addressing this concern to some extent, compliance might either advise on, or be informed of, all reports submitted to regulators. Good practice suggests that they should, at the very least, maintain a central record of all correspondence with the regulator.

Some (usually larger) respondents discuss the effectiveness of their compliance programmes with regulators after report submission. There is also evidence of a forward-looking dialogue in some countries, for example the Netherlands. Some respondents say that they discuss their programme with regulators as frequently as they can. More often, though, one-to-one discussions take place only at the instigation of the regulator and sometimes infrequently, during on-site inspections, for example, or when significant business changes such as mergers or acquisitions take place.

Respondents say that regulatory complexity for group companies increases because of the differences in regulations applicable to different parts of their businesses, and the need to deal with multiple national regulators. Divergences in detailed sectoral rules create particular compliance challenges, and additional cost, for financial conglomerates. In our previous study, differences in regulatory requirements and expectations on a cross-border basis were cited as a considerable cause for concern. Interestingly, a number of respondents to this study note that the introduction of MiFID has reduced concerns in this regard from an EU perspective at least. That said, 36% still see home/host divergence as the most significant or a very significant risk to their organisation and, even in the EU, there is still a perceived need to manage differences in interpretation through direct and indirect dialogue with the regulators concerned.

Dialogue with the host regulators is often entrusted to local compliance officers. Compliance officers in subsidiaries often receive instructions from group Compliance on how to identify and communicate properly any regulatory differences so that group policies can underpin procedures acceptable to both home and host authorities. Internal communication problems

do occur: group Compliance might not have a clear understanding of how to meet the expectations of local regulators. Some respondents flag the need for proactive efforts by group Compliance to appreciate fully the subtlety of local interpretations.

Some believe that the regulatory relationship(s) can be better managed by strong coordination between the group compliance function and compliance representatives in the branches or subsidiaries. A French group indicates that it has formalised this coordination through a service level agreement between group Compliance and the rest of the compliance function.

Finally, respondents indicate that there are also challenges arising from differences in the modus operandi and organisational structure of regulators. Differences in national regulatory approaches could increase compliance resource needs.

‘The new compliance obligations will bring with them an explosion of legal risk’

Table 1

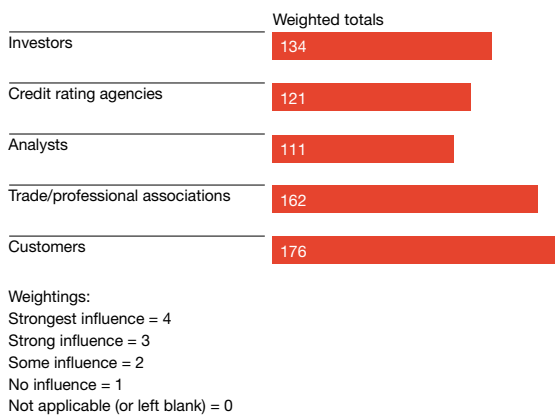
Response to regulator queries	Compliance is often responsible for responding to ad hoc queries from regulators (often by email) either directly, or supporting board or senior management responses.
Contributing to the regulatory agenda	Some respondents actively participate in working groups set up by the regulator or industry associations looking at specific regulatory themes. This is supplemented by individual responses to consultation papers and ongoing dialogue with regulators. A number of respondents stressed regular informal visits with regulator(s) in order to exchange views on compliance themes.
Ongoing dialogue	Most regulators promote a wider exchange of views through industry seminars. Regulators also send questions on specific themes to the industry generally, or to a targeted audience. In terms of MiFID, this has occurred in some countries in relation to conflicts of interest management and inducements. With a risk-based approach to supervision, respondents noted that this may be the only means by which smaller and less risky organisations can maintain an ongoing dialogue with regulators.
Formal meetings	Formal meetings are often held to discuss (annual) reports (in some countries as a ‘trialogue’ with external auditors).
Formal reporting	Respondents generally indicated that the compliance function’s involvement in formal reporting is limited to areas for which it has direct responsibility. The frequency of compliance reporting varies according to the jurisdiction and the issue. Diverse reporting requirements obviously add complexity for groups, and group compliance functions were often responsible for ensuring that all deadlines were met. However, there was evidence of Compliance being consulted on a much broader range of regulatory reports, including prudential reports. Thirty percent were involved in the assessment and quality assurance of the reporting processes, and 33% in defining and implementing reporting process improvements. Twenty-nine percent were involved in ongoing quality assurance, review and testing of regulatory reporting processes and procedures.
Onsite inspections	A number of respondents stressed the importance of compliance’s direct involvement in onsite inspections.
Remediation and crisis management	Many respondents stressed that the business should be responsible for remediation, with compliance function oversight. They also felt that Compliance has a key role to play in crisis management.

Changing expectations of (other) external stakeholders

Clearly, regulators are perceived as the compliance function's most significant external stakeholder. However, customers are also seen as significantly influencing compliance function objectives and activities (see Figure 8).

Figure 8

In addition to the regulators, who are the other external stakeholders who influence the objectives of the compliance function?



Source: PricewaterhouseCoopers

Customer is king

Forty-five percent of respondents see shifting customer expectations as at least a significant compliance risk. They feel that new customer-focused regulations (such as treating customers fairly, customer disclosure and protection requirements) considerably increase legal risks. As consumers become more literate in financial services and aware of their rights, the risk of lawsuits increases with consequent implications for an organisation's reputation. Many respondents expect consumers to seek to enforce their rights more frequently in the future. They note that increased transparency in terms of risk management and compliance practices also magnifies reputation risk, as customers will be able to draw comparisons and react accordingly. Increased transparency of fees and other charges could also impact their organisation's competitive positioning. Respondents feel their firms – and the compliance function – should focus more on the quality of the service to end-customers (not just market intermediaries) as a consequence.

The study indicates that the attention paid by organisations to customer complaints and how they handle them has increased since our previous study. This may reflect growing concerns over service quality or the need to comply with relevant MiFID requirements on complaints handling. The compliance

function's involvement with complaints handling varies significantly. Fifty-nine percent of respondents have a separate complaints-handling department or ombudsman. For others, complaints are handled by another function (for example, legal, internal audit, marketing and public relations, business units, client service teams), depending on the nature of the business and its clientele. Many respondents stress that, although the complaints-handling department or another function takes care of the process, the business is primarily responsible for complaint resolution.

That said, in the majority of cases, the compliance function receives periodic reports, maintains complaint inventories and/or has direct access to a complaints database. The complaints-handling department in some firms formally reports to the compliance function, which is responsible for overseeing the effectiveness of the complaint-handling processes. In others, complaints that present significant compliance risks are systematically reported by the business to the compliance function in line with an established operational risk management framework. The compliance function then oversees the resolution of material complaints by the business unit concerned. In a few cases, however, compliance has no responsibilities regarding complaints handling, is not kept informed of trends or specific complaints and might only become involved in complaint resolution when regulators intervene.

Other external stakeholders

Industry associations are also perceived as influential external stakeholders. Respondents feel that their influence should continue to increase along with their role as a key interlocutor with regulators and as a result of industry self-regulation initiatives.

However, respondents feel that investors, credit rating agencies and analysts are less relevant. Some respondents note potential investor influence in relation to changing ownership structures, a comment that carries significantly more weight now that certain governments have acquired major stakes in some financial institutions. Others voice concerns about the perceived future role of, or expectations of, the compliance function with regard to sustainable business practices and the corporate social responsibility agenda. Some see both the media and external auditors as increasing in influence in the future.

Changing expectations of internal stakeholders

Organisational attitudes towards compliance are improving...

Organisational attitudes to compliance – and compliance functions – appear to have improved since our previous study. Most organisations have positive attitudes to compliance (see Figure 9). Respondents mostly feel that all the statements listed are relevant, with an impressive 96% saying that their organisation wants to manage all risks in the business effectively, including compliance risks. This suggests that compliance functions are increasingly perceived as an intrinsic component of overall governance and risk management systems.

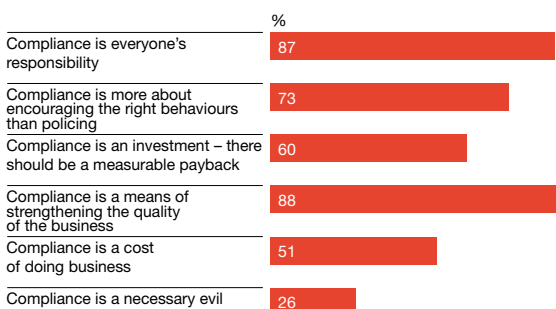
Figure 9
Which statement reflects your organisation's perspective most closely?



6% of respondents did not express a preference. Multiple responses were possible.

Source: PricewaterhouseCoopers

Figure 10
Which statement reflects your organisation's current perception most closely?



Source: PricewaterhouseCoopers

That said, the percentage of positive responses drops by 10% when it is suggested that all business practices and processes should be inherently compliant. It drops even further when respondents are asked if compliance could be achieved cost-effectively (73%) or whether technology could be used to streamline compliance costs (75%). This implies a disconnection between organisations' desire for compliance in theory and the practical implementation of compliance policies and procedures.

...but for some it is still a necessary evil

Respondents were asked to identify which statement (see Figure 10) they feel applies in general to their organisations, and also which they consider the most important. Respondents say that their organisations increasingly see compliance and the compliance function as a means to improve the quality of the business, not just as a cost to be borne. For 24% of respondents, this is their 'most important' consideration. Twenty-three percent of respondents identify 'compliance is everyone's responsibility' as the 'most important' in terms of the attitude of their firm. However, while 73% overall indicate that 'compliance is more about encouraging the right behaviours than policing', this is the first choice for only 8%. Close to a quarter (23%) still feel that (parts of) their organisation saw compliance as a necessary evil, with 11% seeing this as the prevailing perception. This suggests that organisational buy-in is not as strong as it should be in some organisations.

Changing management perceptions...

For some respondents, the establishment of an independent compliance function had been the main driver of change. Other respondents noted improvements in management perceptions as a result of the following:

- Changing board and management perceptions – seeing compliance more as an essential risk management tool rather than an enforced cost
- Growing management attention to ensuring that business processes and procedures are inherently compliant
- Significant investments in risk management and risk control functions generally, and efforts to ensure closer collaboration between them
- Investigation of technological solutions for embedding compliance more effectively
- A better image for the compliance function, moving away from its origins (which are often legal) to become increasingly a recognised partner for business
- Efforts to align compliance practices with international best practice, and to establish or improve national industry platforms for sharing knowledge.

...but management demands can be unreasonable

However, many respondents feel that developing a coherent risk-based approach to compliance across business lines creates complexities that management may not fully understand. This is seen as particularly relevant where the prevailing business culture diverges within a group (for example, between investment banking and private banking, or between banking and insurance).

A number of respondents representing banks express concerns about a potential imbalance in terms of the compliance function's responsibility versus its authority, particularly in relation to the operational risk management function. Some feel that management needs to find a better balance between the often quantitative approach to operational risk management and the more qualitative approach required to manage compliance risk effectively.

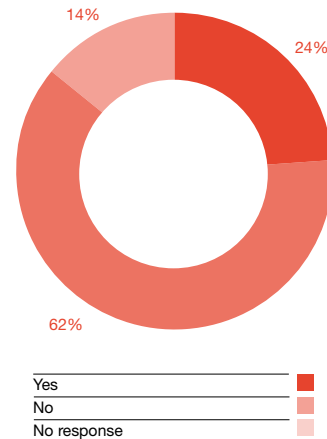
'Best practice standards are illusory: each organisation needs a unique corporate culture and approach to governance and compliance.'

Most importantly, many respondents feel that a specific management expectation that the compliance function address general integrity- and/or reputation risk-related issues can set an unattainable goal. Respondents note that the compliance function cannot be tasked with ensuring compliance with all integrity-based or legally driven requirements to which an organisation is exposed – given the wide scope of these rules and limited compliance resources. Again, the compliance function's potential or current responsibilities in terms of corporate social responsibility are mentioned as a source of concern.

Concerns about the compliance function's remit are heightened by changing or uncertain regulatory (or legislative) expectations of its role when compared with internal expectations and/or a risk-based compliance framework conceived by management. This concern is, for example, evident in relation to the proposed Solvency II requirements, which place potentially wide, but unspecific, expectations on the compliance function. One respondent notes that the broader the definition of compliance, the less effective the compliance function becomes.

A number of respondents suggest that the key challenge results from developing an organisational approach to compliance that is, essentially, tailored to the specific business, operations and structure of each firm. One respondent thinks that 'best practice' standards are illusory when each organisation needs a unique corporate culture and approach to governance and compliance. This can present challenges in demonstrating the effectiveness of the compliance function, both internally and externally.

Figure 11
Do you feel pressure to demonstrate the value of the compliance function?



Source: PricewaterhouseCoopers

Although its perceptions of compliance may have improved, management's growing attention on compliance has begun to lead to questions about the return on its investment from the compliance function. While only 5% of respondents think their organisation considers a measurable payback on the investment as a primary management consideration, 55% think it is definitely a consideration. Respondents mention growing management attention to cost containment (a trend that is strengthening) and the difficulties in balancing potentially large investments in technology against the difficult-to-measure future benefits of increased compliance effectiveness.

While a significant majority (62%) of respondents say they feel no pressure to demonstrate the value of the compliance function (see Figure 11), more established respondents (24%) feel that there is a growing need for the compliance function to demonstrate the value that it brings. This necessitates focused communication within the organisation to emphasise the role of the compliance function in sustainable value creation. Nordic respondents note that such communication could be relatively easy when Compliance has ongoing access to, or forms part of, senior management at the group or business management level, and is seen as an effective advisor providing pragmatic solutions to compliance 'dilemmas'. Nevertheless, Compliance is still looking at quantitative means, such as timesheets and workflow overviews, to reinforce understanding and the perception of its value.

Non-involvement in strategic or tactical decision-making

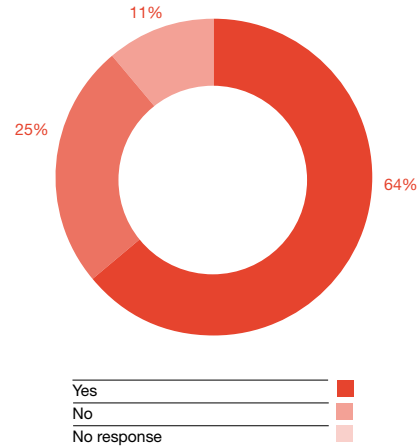
The compliance function's involvement in decision-making processes can be seen as one indicator of the extent to which compliance is embedded within an organisation. Sixty-four percent of respondents said that senior management expected compliance sign-off of all new business and processes, etc (see Figure 12). However, the sign-off requirements are generally in respect of specific products or contracts, rather than wider requirements around businesses and processes. Some respondents also indicate that the requirement is limited to certain types of products. Other respondents participate in, and advise, new product committees, but there is no requirement for approval or sign-off.

Forty-six percent believe that the compliance function is perceived, at least partially, as a contributor to strategic objectives through its advisory activities and the creation of a 'compliance footprint' within the organisation. One respondent notes that its contribution includes the setting and enforcing of clear lines of responsibility and accountability throughout the organisation (for example, a clear management structure, board committees, etc). Only one respondent categorically states that it is seen to contribute to strategic objectives through its compliance risk assessment, prevention and management activities. One respondent notes that Compliance is seen more as a contributor to operational rather than strategic objectives.

However, 42% of respondents do not feel that management sees the compliance function as a contributor to strategic objectives, including wider governance initiatives. For some recently established functions, there is a suggestion that this perception will develop over time. A number of respondents feel that the compliance function should be more involved in corporate governance issues. However, for the majority, corporate governance remains the responsibility of another function, often the company secretary or the legal department.

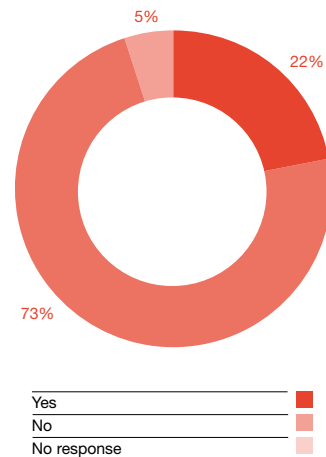
While senior management might not always perceive Compliance as a key advisor strategically, it generally does not see the function primarily as a control function (see Figure 13). Seventy-three percent say that senior management sees the compliance function's responsibilities as including the promotion of business ethics and a compliance culture (see Figure 14). However, while this perception may hold true at the group level, business management teams are more likely to see Compliance as a control function.

Figure 12
 Are there senior management expectations for compliance sign-off of all new business, processes, etc?



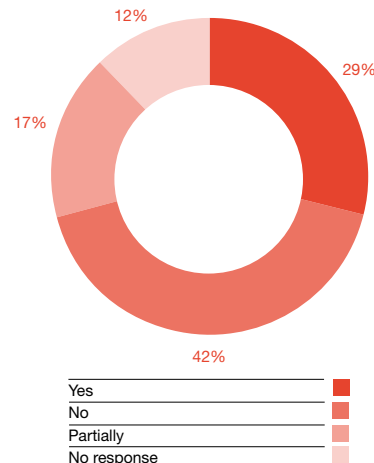
Source: PricewaterhouseCoopers

Figure 13
 Does senior management consider compliance as primarily a control function?



Source: PricewaterhouseCoopers

Figure 14
 Does senior management see compliance as a contributor to strategic objectives?



Source: PricewaterhouseCoopers

Independence of the compliance function in practice

Although larger, more internationally active financial institutions established independent compliance functions well before MiFID, and certain countries had already introduced rules in this regard, this wide-ranging piece of legislation has driven the introduction of compliance functions more broadly. With the impending introduction of Solvency II, this will soon be a regulatory requirement across all financial sectors in the EU. Regulators have provided guidance on what they believe an independent compliance function means in practice. However, there are clearly challenges in balancing the function's independence with its role as a trusted advisor to the business. The dichotomy is, essentially, between not being influenced while being able to influence. The study suggests that, for many, this is still an ongoing dilemma.

'Independence: the state or quality of being independent; freedom from dependence; exemption from reliance on, or control by, others; self-subsistence or maintenance; direction of one's own affairs without interference.'¹²

Webster's Dictionary.

When assessing independence, some key areas to consider include:

- Seniority and profile of compliance officers
- Influence of internal stakeholders
- Configuration of the compliance function and reporting lines
- Clarity of objectives, roles and responsibilities and, importantly,
- Control of own resources.

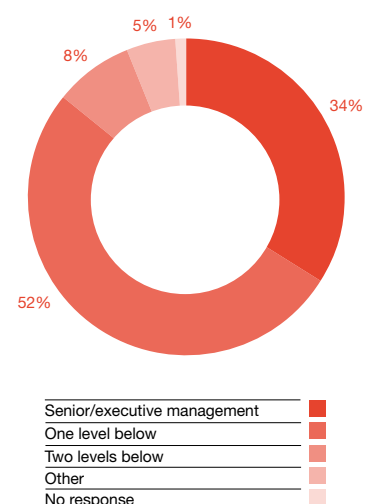
Seniority and profile of compliance officers

The organisational 'clout' and credibility of compliance officers is crucial to their ability to influence commercial decisions appropriately. Seniority is important in this regard: 86% of respondents indicate that the highest ranking compliance officer is either at the level of senior/executive management or, as is more often the case, one level below (see Figure 15). The group compliance officers among the respondents are generally one level below. Thirteen percent of respondents, however, indicate the compliance officer is less senior than this.

'Fit and proper' requirements can provide external reinforcement for a compliance officer's credibility. These currently apply infrequently to compliance officers: only 39% of respondents say that there are national requirements in this regard (51% say there are none). Where such requirements do exist, supervisors in some countries receive information prior to an appointment and have the opportunity to comment before the appointment is confirmed. Elsewhere, firms need only inform the supervisor of appointments (and the supervisor may keep a register). Most countries require supervisors to be notified if a compliance officer is dismissed or resigns.

There is growing recognition that the compliance function needs an increasingly diverse set of skills to meet its broad objectives. Respondents stress that there is no specific profile for a compliance officer. Many still consider a legal background preferable for compliance officers since this positions them well, in the business's eyes, to provide advice (when combined with deep industry and organisational knowledge). However, compliance functions also need other skills, including: audit and internal control experience; forensic skills to deal with AML and fraud investigations; risk management expertise; financial and accounting skills; and IT knowledge. There is a wide expectation among respondents that compliance staff will be university graduates or have business experience.

Figure 15
What is the level of seniority of the highest ranking compliance officer?



Source: PricewaterhouseCoopers

Many respondents stress the importance of compliance officers having the correct character. Above all, they need integrity, discretion, common sense and a strong 'moral compass'. Effective communication and influencing skills are also seen as essential.

Only 4% of respondents refer to management skills, including project management skills, as key for compliance officers. However, clearly such skills are required to run a sizeable compliance function, implement major compliance projects (see page 39) and manage a function that possesses such a diverse skills-set.

Influence of internal stakeholders

Various internal stakeholders influence the objectives of the compliance function (see Figure 16). However, respondents note that this influence can be 'active' or 'passive', or somewhere between the two.

Figure 16
Who are your key internal stakeholders and how strong is their influence on the objectives and activities of the compliance function?



Weighting:
Strongest influence = 3
Strong influence = 2
Some influence = 1
No influence and not rated = 0
[100% response rate]

Source: PricewaterhouseCoopers

Overall, respondents see the board of directors as the most influential stakeholder, slightly more influential than senior management: 83% rank the board of directors as having the strongest or a strong influence, compared with 80% for senior management. Seventy percent of respondents indicate that the

board is the body ultimately responsible for compliance (49% of respondents have a board committee responsible for compliance). Twenty-eight percent indicate that senior management is ultimately responsible for compliance.¹³

Internal audit is rated the third most influential internal stakeholder: 66% say it has the strongest or a strong influence, often reflecting its responsibilities for reviewing the effectiveness of an organisation's wider control framework. Internal control is also rated relatively highly where a separate internal control function exists. The legal department is considered more influential than both business management and risk management.

The public affairs/government relations department is seen as the least influential overall: only 12% indicate that it has a strong influence on compliance function objectives. This may affect the consistency of communications with legislators and regulators. It can also raise questions in terms of wider communications with the markets and customers. However, this finding could reflect the fact that the compliance function exerts influence on the objectives/activities of the public affairs/government relations department, rather than vice versa.

Complaints handling and customer service are rated higher than the human resources (HR) function, but only 22%, 18% and 14%, respectively, say that these departments have a strong influence. In terms of complaints handling and customer service, these results appear to diverge from the conclusion reached earlier – that more attention needs to be paid to the quality of customer service. Here again, however, it might be expected that the compliance function has a stronger influence on the objectives of these functions, than vice versa. A similar argument may apply to HR: however, the results may also raise questions about the degree of collaboration between the two in terms of developing and embedding a compliance culture on an ongoing basis. This issue is revisited later in this report.

Organisation of the compliance function and reporting lines

Common structures

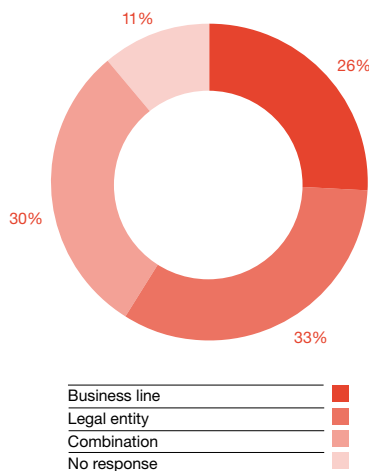
The majority of respondents have either a centralised structure (41%) or a combination of centralised and decentralised (42%) for the compliance function. A centralised structure entails direct, hierarchical reporting within the compliance function: a decentralised structure entails 'dotted line' reporting. The most common approach, particularly among the larger, multi-business and multinational respondents, is to adopt a matrix structure with a group compliance function supported by a network of compliance officers within business lines and/or at entity level, or compliance 'agents' (or antennae) in branches.

¹³ This includes the German respondents. It should be noted that German law stipulates that the compliance function is the responsibility of the Vorstand, or executive committee, which forms part of the two-tier corporate governance system in Germany.

Often, the group compliance officer (and function) has direct reporting lines to the board of directors and/or senior management at the group level, while business line and entity compliance officers report directly to business line management or the entity CEO, and functionally to group Compliance. While there are some examples of a functional reporting structure – with all business compliance staff reporting directly within the compliance structure itself – these are definitely in the minority and generally related to smaller, more ‘monoline’ organisations. Business compliance officers and staff are generally employed by the business (at entity level) rather than the compliance function. In smaller organisations or entities, compliance responsibilities are often split between compliance and another control function, such as legal or risk management.

Views on the optimal approach for the compliance function differed. Given the importance of national legislation, a third of respondents feel that the structure needs to be organised on a legal entity basis, while 24% feel it is better to organise compliance along business lines. One third – again mostly larger, more diverse organisations – feel that the optimal structure should combine both business and legal dimensions. There is a slight discrepancy from the actual structures (see Figure 17). While the majority believe that their current structure does not impede the effectiveness of the compliance function, 27% feel barriers exist.

Figure 17
How is your compliance function currently structured?



Source: PricewaterhouseCoopers

Compliance policies

Common compliance policies are widely used to strengthen the compliance framework and promote consistency in approach throughout an organisation. Seventy-one percent of respondents indicate that they have an overall compliance policy (sometimes due to specific national regulatory requirements – in Belgium and Luxembourg, for example). An overarching compliance policy can define the role – and influence – of the compliance

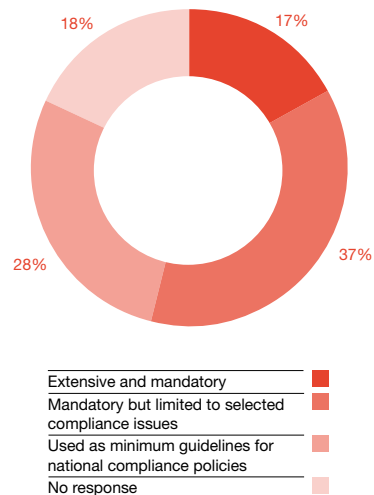
function. For many international respondents an overarching compliance policy, adopted by the board at group level, provided the backdrop for (all) other compliance-related policies within the group. However, there are various documents – with different purposes – that are mentioned by respondents in relation to an overall compliance policy:

- A compliance charter that establishes the objectives and modus operandi of the compliance function
- A (group) compliance policy, alternatively called a Code of Ethics, Code of Conduct, etc., which pitches the board’s expectations in terms of management and staff behaviour throughout the organisation
- A board-approved (group) policy that sets out the compliance risk management approach within the organisation, establishing its compliance ‘risk appetite’
- A combination of compliance policies dealing with specific business areas or regulatory requirements, potentially combined into compliance manuals (see below).

Only the first of these sets clear parameters for the scope and approach of the compliance function.

Eighty-two percent of respondents indicate that the compliance function is responsible for setting group and/or business-line compliance standards and policies. For 54%, these compliance policies are mandatory (see Figure 18); for 17%, they are both mandatory and extensive. Respondents say that changes to mandatory policies at the local level are generally only possible if resulting from specific national regulatory requirements. For 28%, the policies establish minimum compliance standards. Here too, though, group compliance functions often require information on the nature of, and reason for, any deviation and monitor implementation through frequent reporting.

Figure 18
If group/business compliance policies are applied, how would you describe these?



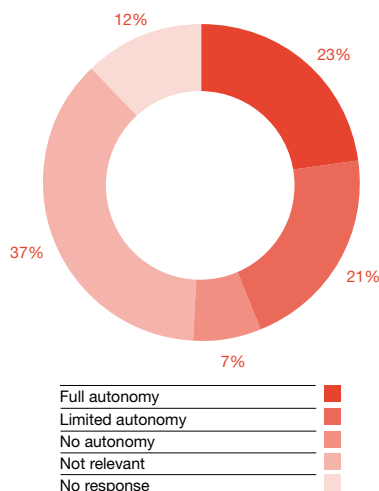
Source: PricewaterhouseCoopers

The compliance function is most often seen as responsible for communicating the various policies and associated procedures. Communication of these policies is generally 'passive' via employee induction packs, intranet, emails, training sessions and ongoing advice from Compliance. Some respondents say that executives are required to confirm in writing, at regular intervals, that they have read, understood and applied relevant policies appropriately. A few respondents, however, believe that this communication needs to be part of a structured internal communication exercise driven by management, supported by the HR and internal communications departments (where appropriate), as this is a critical mechanism for embedding a compliance culture and promoting the influence of the compliance function.

Autonomy of subsidiaries and branches

In terms of the autonomy afforded to subsidiaries in carrying out their compliance responsibilities (see Figure 19), there is an almost even split between those with full autonomy (23%) and those with limited autonomy (21%), with 7% indicating that subsidiaries have no autonomy (i.e. decisions are driven by group Compliance). Whether full or limited autonomy, respondents say that group policies provide essential guidelines. Some indicate that autonomy is essentially limited by the overall coherence of the compliance function throughout the group; others say that implicit boundaries to autonomy result from the consistent application of key group policies or initiatives spearheaded by group Compliance (for example, MiFID and AML).

Figure 19
 To what extent do (overseas) subsidiaries have autonomy in carrying out their compliance responsibilities?



Source: PricewaterhouseCoopers

In terms of branch networks, the integrity of the compliance approach is reinforced through regular information-sharing sessions and reporting, continuous cooperation and advice, circulars, common controls and testing, and periodic refresher training sessions. Periodic onsite visits are also mentioned frequently in the responses. One respondent emphasises the

importance of technology in facilitating communication and control throughout branch networks.

Branches often form the main axis in a matrix structure, with business line compliance and local compliance personnel working in close parallel. Again, the application of group policies can determine day-to-day approaches at the branch level (monitoring programmes, for example). One respondent notes that the approach at branch level is complex as it is derived, inter alia, from risk-mapping exercises done centrally with ex-ante validation of processes, products, structures and projects at the branch level. Another stresses the need to communicate adequately the risks of non-compliance in the branch, together with the back-up mechanisms of a whistle-blowing programme and internal audit reviews.

Outsourced functions and activities

There are strong parallels in approach in terms of controlling third-party networks and outsourced functions or activities. Key control elements stressed by respondents include:

- Quality of the due diligence exercise prior to entering the relationship
- Contracts and written agreements (service level agreements)
- Robust monitoring by the (local) compliance function and testing exercises (for example, mystery shopping)
- Ongoing communication and training sessions
- Metrics/controls/reporting
- Quality of the compliance function within the third-party distributor or outsourcer, and compliance policies in place, as well as a clear definition of compliance processes
- Onsite reviews by compliance and internal audit
- Complaints analysis
- Dedicated unit within the compliance function to oversee third-party distributors or outsourcers.

That said, a number of respondents still feel that ensuring compliance by either third-party distributors or outsource service providers is not easy. Some are concerned that their organisation's approach in this regard is suboptimal.

Reporting

Seventy-eight percent of respondents say that the compliance function's reporting lines are formally documented and communicated throughout the organisation, often by means of the firm's intranet.

Forty-four percent report directly to the board of directors and a further 31% via a board committee (generally the audit committee), while 25% report to the board via senior management. In some cases, quarterly reports to the relevant board committees are supplemented by annual reports to the full board. In terms of frequency (see Figure 20), 47% report to the board on an annual or semi-annual basis, and another 38% on a quarterly basis. Those with even more frequent reporting are generally medium-sized firms or entities within major groups, apart from one large Spanish bank.

In smaller organisations, informal contacts with the board are also often easy, through email, phone calls or face-to-face discussions, even on a daily basis. In larger organisations, although group compliance officers often have frequent informal contacts with members of the group board or board committees, access to boards at entity level within the group more widely may be limited. Only 32% of respondents say that they can access the board whenever needed. A small minority (8%) have no direct formal or informal contacts with the board.

Thirteen percent of respondents report to (senior) management on a formal basis only (see Figure 21); 69% report both formally and informally. Three percent report to senior management only informally and 15% report exclusively to the board. Formal reporting to senior management is more frequent than to the board: 51% report to senior management on a quarterly or more frequent basis (see Figure 28).

Clarity of objectives, roles and responsibilities

Scope of the mandate

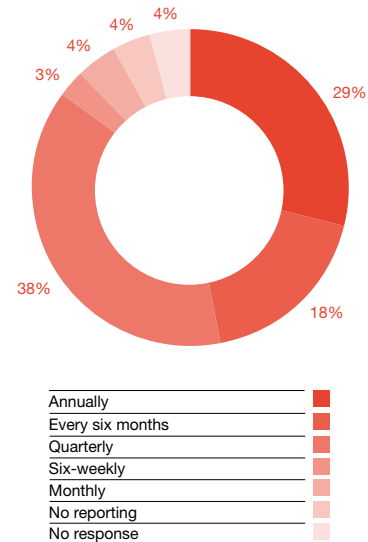
The scope of the mandate of compliance functions diverges considerably, not simply as a result of varied regulations applying to different businesses (see Figure 22). Divergence in scope is sometimes a consequence of specific national legislation: for example, compliance functions in Belgium are required to oversee compliance with the rules against ‘special mechanisms’ (relating to the tax evasion) and the independence of statutory auditors. However, the disparity goes beyond this.

Traditionally, compliance functions have focused on the conduct of business in terms of market and customer-facing activities and issues. A number of respondents indicated that the compliance function is becoming more involved – or expects to be soon – in prudential issues, albeit in an advisory capacity. Compliance functions are also getting more involved in internal and external fraud prevention measures, as these relate to integrity- and ethics-related initiatives. AML compliance officers are now frequently seen as an integral part of the compliance function (as opposed to working in parallel). Although the majority of respondents (64%) say they are not involved in sustainability and/or value reporting, 17% are, and a further 3% expect to be in the future.

‘A clear and limitative definition of integrity, specific compliance domains and compliance tasks (monitoring and reporting) would make the compliance function much more efficient and effective.’

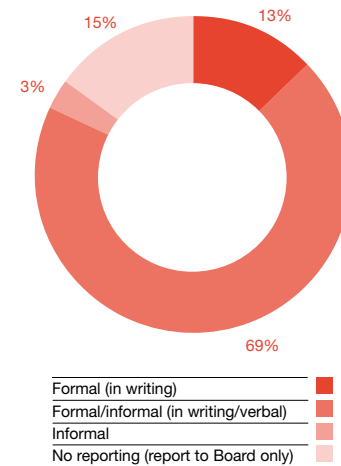
These results are symptomatic of a general trend to broaden the role of the compliance function, in line with the objective of managing reputation risk, and the recognition that a breach of

Figure 20
How frequently does the compliance function submit a formal report to the board?



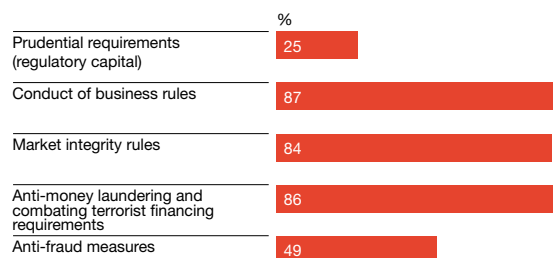
Source: PricewaterhouseCoopers

Figure 21
How does the compliance function report to senior management?



Source: PricewaterhouseCoopers

Figure 22
What is the scope of the compliance function’s responsibilities?



Source: PricewaterhouseCoopers

any regulation to which the organisation is subject can damage reputation. For some, there is a temptation to expect the compliance function to get involved in all areas, without necessarily increasing resources in line with these expectations. One respondent notes: *‘the systematic ‘marketing’ of the compliance function (creating needs which did not exist yesterday) only results in a continuous addition of new roles and operational tasks for the compliance function. This – accompanied by an extremely vague definition of ‘integrity’ – will, in the end, suffocate a lot of compliance functions which systematically have to do more with the same means’.*

Clarity of objectives

The vast majority of respondents (86%) say the objectives of the compliance function are clearly established in a compliance charter or similar. In addition, respondents note that compliance function objectives can be explicitly or implicitly established through various mutually reinforcing mechanisms, which, in addition to the documents mentioned on page 33, can include:

- Annual compliance management plan
- Individuals’ job descriptions
- Performance objectives, both in terms of the compliance function as a whole and personal objectives (compliance function and broader employee base)
- Charters clearly delineating the objectives of other functions (legal, risk management, internal control, internal audit).

Overall, the four highest ranking objectives (see Figure 23) mirror the results of our previous study. In addition to those listed, other objectives specifically mentioned include:

- Influencing the regulatory agenda and lobbying in relation to proposed legislation
- Stimulating compliance awareness and conviction within the organisation
- Looking after customers’ interests

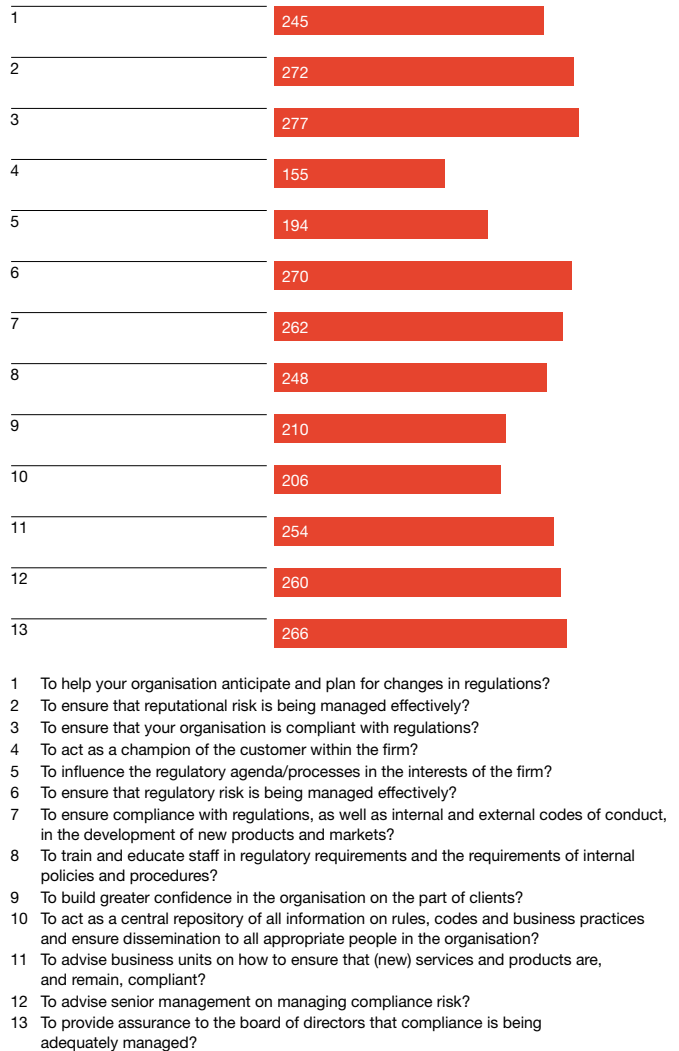
All of which clearly echo earlier reflections in this report.

Individual objectives and roles

Sixty-three percent of respondents have established personal objectives for the compliance team as a whole, or are working towards this. In some cases, however, personal objectives exist only for more senior compliance personnel or may need to be further personalised for the staff member concerned. Some respondents note that the objective-setting and evaluation cycle used in the compliance function is aligned to the appraisal process adopted throughout the organisation. Fifty-six percent say that the objectives are reviewed annually. For the majority of the remainder, objectives are reviewed every six months or when the need arises (see Figure 24).

The majority of compliance officers have job descriptions, but this does not always apply to the whole compliance function. The gap has sometimes been filled through documenting the various tasks/roles to be undertaken by compliance staff, possibly at the unit or subunit level (for example, in terms of difference monitoring activities at branch level).

Figure 23
In your view, what are the objectives of the compliance function (in its broadest sense) within your organisation?



Weightings:
Very important = 4
Important = 3
Of lesser importance = 2
Not important = 1
Not rated = 0

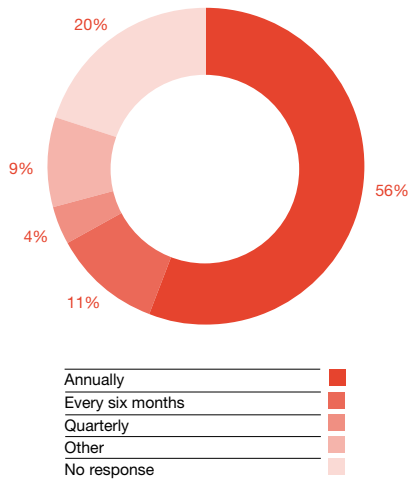
Source: PricewaterhouseCoopers

Consistency of functional versus organisational objectives

Asked whether the expectations of the other risk and control functions are broadly in line with the objectives of the compliance function, 70% feel they are. In some of the more mature compliance environments, clarity was ensured through formal agreements relating to objectives and roles of different risk and control functions (including risk management, internal control and internal audit). However, 20% feel the objectives are not aligned – or not completely – with the expectations of these risk and control functions.

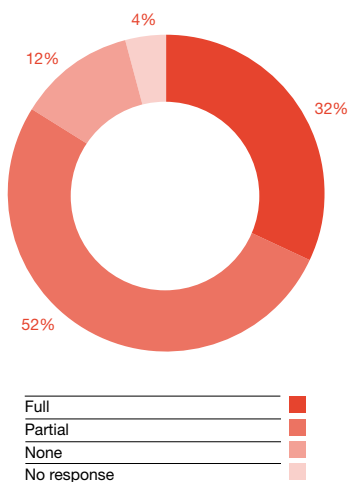
Sixty-three percent of respondents (and not exclusively newly established compliance functions) feel that business units’

Figure 24
How frequently are compliance function objectives reviewed?



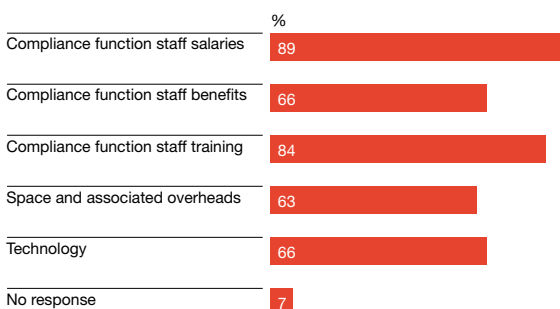
Source: PricewaterhouseCoopers

Figure 25
Does the compliance function have full or partial discretion on how it spends its budget?



Source: PricewaterhouseCoopers

Figure 26
What does the budget cover?



Source: PricewaterhouseCoopers

expectations do not always mesh with compliance functions' objectives. Business units sometimes expect the compliance function to address issues related to any applicable legislation, including labour laws, for example, rather than its narrower remit. Some feel that this can result from a compliance culture being insufficiently embedded within the organisation. Others suggest that these differences in perspective may result from business units' commercial mindset – the compliance function is not always seen as a natural participant in the product development process, for example. Issues can also arise from a lack of knowledge and understanding of the allocation of compliance responsibilities between different functions, or where the compliance function is expected to supplement insufficient skills or resources in operational units.

Control of own resources

Thirty-two percent of respondents have full discretion over the management of their budget (within the context of a compliance management plan) (see Figure 25). The largest percentage (52%) had partial discretion, with decisions on non-discretionary expenditure generally taken by a member of senior management or the executive committee (including CEO, CFO, CRO and resource director) either at group, business or entity level, or by the board or relevant board member. In some organisations, such decisions are taken by more senior members of the (group) compliance function. In others, however, Compliance is still a formal part of the legal or other department without a separate budgetary allocation. Twelve percent of respondents indicate that the compliance function has no discretion over its expenditure.

Over 80% of compliance budgets cover compliance function staff salaries (89%) and training (83%), although, in some cases, training falls under a general HR budget (see Figure 26). Overheads and technology are more frequently part of a central or local budget for internal support functions or IT departments (sometimes with reallocation). The salary and training costs of compliance staff embedded in the business are included in the compliance function budget in only 20% of cases; budgets for 'embedded' compliance staff are generally established by the business division or entities concerned.

In some cases, Compliance headcount needs to be ratified first by local management and then by group Compliance/head office. Certain respondents, with separate compliance budgets at group and division level, note that some costs (for example, compliance measurement/awareness instruments) for divisions are included on group budget in its capacity as the coordinating body.

Forty-three percent of respondents indicate that where different budgets cover the activities of the compliance function, it is clear which budget applies in given situations (17% indicate that it is not clear). Where there is a budgetary split, 17% also say that this could create difficulties with mobilising resources when needed.

The scope of compliance function activities

Asked how members of their compliance function spent their time, 65 respondents provide detailed activity breakdowns for compliance officers and 51 for compliance staff. This implies that there may be less understanding among respondents of how compliance staff use their time and/or that activity statistics for the compliance function as a whole are not often compiled.

At the aggregate level, the results do not reveal any major surprises. However, variations are significant at the individual institution level. In terms of activities (see Table 2), compliance officers generally spend more time than compliance staff in advising the business, interfacing with regulators, promoting the adoption of the compliance culture, developing the compliance function's role and initiating and taking preventative measures. Compliance officers generally initiate compliance projects or activities, while compliance staff support their compliance officers and the business. On average, compliance function staff spend more time than compliance officers on:

- Monitoring compliance with regulations and internal policies and procedures
- Monitoring regulatory developments and their impact on the organisation
- Participating in new business approval processes
- Taking and monitoring remedial or corrective measures, and
- Training and education of business units.

This suitably reflects a distinction between compliance staff activities versus the more senior compliance officers.

However, comparing the results of continental European organisations taking part in our previous study, there are some notable differences. Average time spent on establishing compliance policies and procedures has dropped significantly, from 22% to 10%. As most respondents to this study have compliance policies and procedures in place, their focus now is on maintaining them.

Interestingly, time spent on providing advice to management and the business has also dipped significantly, while the focus on taking and/or monitoring remedial or corrective measures and initiating and taking preventive measures have both witnessed a significant increase in the past three years. This may be a result of the introduction of MiFID and, although not conclusive, suggests improved understanding and awareness of compliance risk management requirements by the business generally, and a more proactive approach by the compliance function towards preventive measures.

While there is little change in terms of time spent promoting the adoption of a compliance culture within the organisation, attention to further developing the role of the compliance function has increased. All of the above suggest an increasing maturity in the approach to compliance risk management.

Comparing the responses of group compliance officers to those of compliance officers in subsidiaries, the distribution of effort is closely comparable in terms of the average time spent (see Table 3). On average, group compliance officers spend marginally more time on:

- Interfacing with regulators
- Establishing compliance policies and procedures
- Taking/monitoring remedial or corrective measures
- Further developing the compliance function's role
- Initiating and taking preventative measures.

In subsidiaries, compliance officers on average spend more time than their group counterparts on:

- Monitoring compliance with regulations and internal policies and procedures
- Monitoring regulatory developments and assessing the impact on the organisation
- Participating in new business approval processes
- Training and education of business units.

That said, when comparing the average time spent by compliance officers working in the larger organisations participating in the study, there is a notable difference in terms of time spent on various activities. In larger organisations, compliance officers spend more time reporting to senior management, in interfacing the regulators and in initiating and taking preventive measures. They spend less time monitoring regulatory developments and assessing the impact on the organisation and even less time on monitoring compliance with regulations and internal policies and procedures. However, they also spend more time in promoting the adoption of a compliance culture and in further developing the compliance function's role.

In addition to the listed activities, (group) compliance officers in some of the larger organisations say they spend a considerable percentage of their time managing the compliance function (over 20%). It is notable however that only 4% of respondents mention this time commitment. Other activities identified by one or more respondents include participation in decision processes in relation to ongoing business (account opening, loans, AML, etc.) and cooperation with police and intelligence units.

Table 2

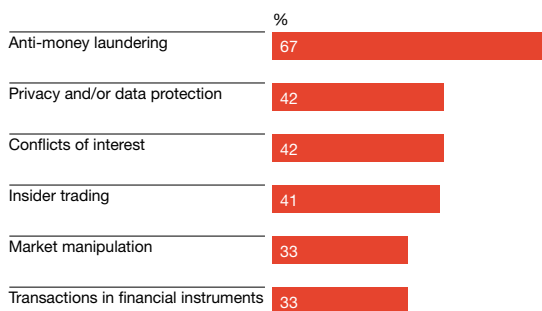
Average time spent	Compliance officer	Compliance staff	2005 results (Cont Europe)
Monitoring compliance with regulations and internal policies and procedures	13%	21%	10%
Reporting to the board/senior management	7%	4%	5%
Monitoring regulatory developments and assessing the impact of the organisation	10%	12%	13%
Providing advice to management and to business generally	12%	11%	22%
Participating in new business approval process, including new products, new markets, mergers & acquisitions	7%	8%	6%
Interface with regulators	6%	3%	5%
Establishing compliance policies and procedures	10%	10%	22%
Taking/monitoring remedial or corrective measures	5%	7%	2%
Training and education of the business units	7%	9%	6%
Promoting the adoption of a compliance culture within the organisation	6%	4%	6%
Further developing the compliance function's role	6%	3%	2%
Initiating and taking preventative measures	7%	5%	1%
Results do not total 100% due to some firms including activities in the 'other' category.			

Table 3

compliance officer time	Average time spent	Large organisations	Group/ parent	Subsidiary
Monitoring compliance with regulations and internal policies and procedures		7%	12%	14%
Reporting to the board/senior management		8%	7%	6%
Monitoring regulatory developments and assessing the impact of the organisation		9%	10%	11%
Providing advice to management and to business generally		12%	12%	12%
Participating in new business approval process, including new products, new markets, mergers & acquisitions		7%	6%	8%
Interface with regulators		7%	6%	5%
Establishing compliance policies and procedures		9%	10%	9%
Taking/monitoring remedial or corrective measures		5%	6%	5%
Training and education of the business units		5%	7%	8%
Promoting the adoption of a compliance culture within the organisation		10%	6%	6%
Further developing the compliance function's role		9%	7%	4%
Initiating and taking preventative measures		8%	7%	6%
Results do not total 100% due to some firms including activities in the 'other' category.				
Large organisations: the 16 largest organisations participating in the study (all with market capitalisation – or equivalent – above €100bn). Six groups/parents and four subsidiaries did not respond to this question.				

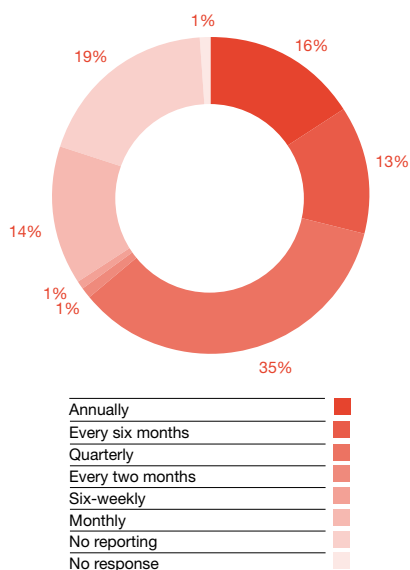
There is clear evidence of specialisation within compliance functions. Sixty-seven percent of respondents have dedicated AML compliance officers (see Figure 27). Additionally, 42% have compliance officers dedicated to privacy and data protection; 41% have personnel dedicated to monitoring insider trading; and 33% to market manipulation. With the introduction of MiFID, 33% now have compliance staff focusing exclusively on reporting transactions in financial instruments and a significant 42% on conflicts of interest management. Twenty-nine percent also have compliance staff dedicated to information technology (in the majority of cases, IT security remains the responsibility of the IT department). Other areas of specialisation identified include personal account dealing, best execution, products and services, complaints management, and anti-corruption.

Figure 27
Do you have dedicated compliance officers in specific areas or for specific issues?



Source: PricewaterhouseCoopers

Figure 28
How frequently does the compliance function submit a formal report to senior management?



Source: PricewaterhouseCoopers

Monitoring compliance with regulations and internal policies and procedures

The amount of time spent by compliance officers in compliance monitoring activities varies significantly. Although the average was 13%, a number of respondents indicate that they spend more than 20% of their time on compliance monitoring (in one case 35%). The average time taken by compliance staff for compliance monitoring is 21%, with a range from 0% to 60%.

It is not necessarily the case that higher involvement in compliance monitoring is directly related to the size of the organisation and the compliance resources in place. In larger organisations, responsibility for compliance monitoring is often delegated to compliance staff or specialist units within the compliance function and the involvement of (group) compliance officers is significantly lower. However, seven of the largest groups in the study indicate that their compliance officers spend more than 10% of their time on monitoring-related activities.

The scope of monitoring is discussed further in the next section of this report. Different regulatory obligations (for example in different sectors) impact the extent and type of compliance monitoring activities. Sixty-five percent of respondents say that compliance monitoring activities are designed to assess the organisation's compliance with considerations that are broader than pure regulatory requirements, including industry codes, internal policies and international best practice. However, the focus of compliance risk assessments is primarily on specific regulatory requirements. Respondents indicate that monitoring requirements are, in general, derived from these risk assessments.

Reporting to the board and senior management

In terms of reporting to the board/senior management, compliance officers' involvement ranges from 0% to 20% of their time, with a mean of 7%, although it can take up as much as 15% of their time. However, in many cases compliance staff have no responsibilities in relation to reporting. The difference in time spent may be explained by differences in the type of reporting and the frequency of reports (see page 35).

Monitoring regulatory developments and assessing the impact on the organisation

Compliance officers spend between 0% and 30% of their time monitoring regulatory developments and assessing the impact on the organisation, with a mean of 10%. For compliance staff, the range is between 0% and 50%, with a mean of 12%. Responsibility for monitoring upstream regulatory risks is often shared with the legal department. Some respondents have specialist units focusing on monitoring regulatory developments, lobbying regulators as appropriate, and preparing the organisation for the resulting changes.

Providing advice to management and to business generally

Ninety-six percent say that Compliance is available on an ongoing basis to provide guidance and advice to business units and employees on ethical and compliance-related issues. This is often through dedicated mailboxes or an 'open door' policy (31% have a formalised helpline). Time spent by compliance officers ranges from 1% to 33%, with a mean of 12%. Compliance staff spend between 0% and 30%, with a mean of 11%.

Participating in new business approval processes, including new products, new markets mergers and acquisitions

The range of time spent by compliance officers providing advice on new products, processes and markets or mergers and acquisitions is between 0% and 30%, with a 7% average. For compliance staff, the range is between 0% and 30%, with a mean of 8%.

As seen earlier, 64% of respondents indicate that senior management expects compliance officers to participate in new product approvals, sometimes with the right of veto. The level of involvement in the decision-making processes ranges from 'no involvement' to 'leading role'. Essentially, the nature of the involvement encompasses approval, through recommendations and opinions, to the review and sign-off of the relevant documentation. For the majority, formal involvement appears limited to new product approvals, rather than new markets and processes, and mergers and acquisitions. Compliance officers are increasingly members of new product approval committees; some are actively involved in due diligence processes as a result, while others advise the committee.

Table 4
Examples of (group) policies

Accuracy of disclosures	Internal fraud
Advertising	Investigation and litigation
Anti-market timing and related issues	Outside directorships and other outside activities and interests
Antitrust and fair dealing	Outsourcing
Best execution and client order handling rules	Political contributions by or on behalf of group companies
'Chinese' or ethical walls	Procurement
Clear desk	Product approval procedure
Cold calling and mailing	Producer distributor
Confidentiality	Protection and proper use of group assets
Conflicts of interest	Quality of staff
Customer due diligence	Record keeping and retention
Customer complaints	Regulatory inquiries
Data protection	Relationships with government personnel
Employee complaint handling	Reporting breaches to regulators
Employment screening	Reporting misconduct and whistle-blowing
Fund governance	Sanctions and embargoes
Gifts, entertainment and inducements	Secrecy and privacy rules
Improper influence on conduct of audits	Trading
Individual conduct	Valuation
Insider trading	

Another area where there is clear involvement is in respect of client take-on procedures, with compliance officers participating regularly in client acceptance committees (a number of respondents highlight that this has resulted from the introduction of MiFID).

Interface with regulators

Interaction with regulators is discussed in detail on page 25. For compliance officers, time spent ranges between 0% and 15%, with an average of 6%. For compliance staff, the range is between 0% and 10%, with an average of 3%.

Establishing compliance policies and procedures

For compliance officers, the range of time spent on this activity is between 0% and 25%, with an average of 10%. For compliance staff, time spent ranges from 0% and 20%, again with an average of 10%.

The majority of respondents indicate that the compliance function is deemed responsible, with board approval, for developing and rolling out compliance policies. Obviously, different policies are needed for different types of business. However, even when taking this into account, the coverage and nature of group or business-specific policies varies significantly (see Table 4). This may, of course, reflect different levels of maturity in the compliance structures of the participants.

The frequency of review depends on the nature of the policy. However, the majority of respondents undertake an annual reassessment or when a significant event has occurred.

Taking/monitoring remedial or corrective measures

For compliance officers, time spent ranges from between 0% and 10%, with an average of 5%. For compliance staff, the range is between 0% and 25%, with an average of 7%.

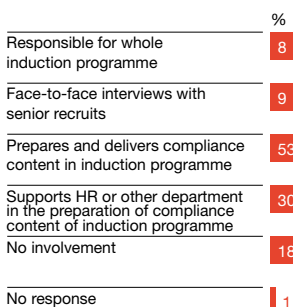
A divergence in compliance's scope of responsibility was noted here. Just under half of respondents (49%) specify that the business unit responsible for the breach is also responsible for its rectification, while the compliance function advises and oversees rectification. Nineteen percent of respondents indicate that the compliance function is responsible for both rectifying breaches and overseeing their rectification. A further 5% indicate that the compliance function is responsible for rectifying breaches and is overseen by another function – such as internal audit – or by management. Other respondents indicate that rectification and oversight are the responsibility of the board and/or senior management, or functions such as the legal department, risk management or internal audit.

Training and education of the business units

For compliance officers, training and education of business units takes between 0% and 33.3% of their time, with an average of 7%. For compliance staff, the range is between 0% and 40%, with an average of 9%. Specific training and education activities primarily relate to the induction of new staff, staff 'refresher' sessions, and training related to specific or new regulatory requirements and/or internal policies.

The extent and focus of an induction programme, and the compliance function's involvement (see Figure 29), can vary depending on the nature of the business (as well as the type of employee). Fifty-three percent of respondents indicate that they prepare and deliver the compliance content of the induction programme. Twenty-nine percent say that they support HR in the development of the entire induction programme, and a further 8% that the compliance function is responsible for the induction programme as a whole. Only 9% indicate that they are involved in the face-to-face induction of senior recruits (for example, portfolio managers). Induction packs may be provided in lieu of, or in addition to, specific training.

Figure 29
What role does the compliance function play in the induction of new staff?



Source: PricewaterhouseCoopers

Staff refresher sessions focus on specific regulatory requirements. In particular, many respondents noted that refresher training is held regularly on AML requirements. New regulatory requirements, such as MiFID, market abuse, etc., can also necessitate fairly extensive training.

Most respondents indicate that the compliance function takes the lead in all compliance training, which may take the form of 'spontaneous' training, organised on an ad hoc basis as the need arises; or a pre-scheduled, pre-planned training programme, which uses a variety of training techniques including e-learning; or a combination of both. Respondents feel that different approaches are needed for different topics. Two respondents mention the use of quizzes or games to facilitate broad awareness of complex challenges relating to integrity (for example, AML, privacy, conflicts of interest).

'In reality, it is mainly compliance which feels responsible for corporate values/ethics and compliance culture, but, due to low resources, capacity is rather limited'.

Some respondents indicate that, rather than taking the lead, the compliance function collaborates with other functions, providing the structure and content of the training programmes in relation to compliance. One respondent indicates that it is the responsibility of the compliance function to validate all the training processes within the group; another that the compliance function draws up the training manual in conjunction with HR.

Promoting the adoption of a compliance culture within the organisation

For compliance officers, the time spent ranges from 0% to 11%, with an average of 6%. For compliance staff, the range is between 0% and 40%, with an average of 4%. Respondents suggest that Compliance's specific roles in relation to improving the compliance culture include:

- Drafting and distributing codes of conduct and rules of integrity
- Ensuring awareness through induction and ongoing training programmes
- Working in cooperation with other departments/units in strengthening corporate identity and culture
- Advisory role, providing an information centre and an ethical helpline
- Observing behavioural trends within the organisation and developing recommendations for change
- Continuous internal communications
- Facilitating compliance risk assessments, and the investigation and rectification of breaches.

Sixteen percent of respondents say that the compliance function takes the lead in determining changes needed to bring the organisation in line with corporate ethics and values, and/or embedding a compliance culture. Sixty-three percent say they

are involved in different capacities, not least through supporting and advising senior management in implementing changes, or acting as project managers and facilitators. Seventy-eight percent indicate that the compliance function has a role to play in communicating corporate ethics and values throughout the organisation. The role, however, varies from ‘a leading role’ to providing support to the board of directors and/or senior management.

Further developing the compliance function’s role

For compliance officers, the percentage of time spent developing the compliance function’s role ranges from 0% to 30%, with an average of 6%. The higher percentages mainly represent respondents with newly established compliance functions. In established compliance functions, limited time is spent in this respect. For compliance staff, the range is between 0% and 10%, with an average of 3%.

Initiating and taking preventive measures

For compliance officers, the percentage of time spent ranges from 0% to 33.3%, with an average of 7%. For compliance staff, the range is between 0% and 36%, with an average of 5%.

Most respondents stress that the compliance function’s role is preventive. However, such issues as staff shortages, lack of preparation for new regulations, or too many projects through new regulations or rapid group expansion, among others, can result in a more reactive approach to compliance management. Just over a fifth of respondents (21%) confess to ‘fire fighting’ (see Figure 30). This is not exclusive to newly established compliance functions. In fact, respondents from larger, more complex organisations note that fire fighting is never totally avoidable, as it is difficult to plan for every eventuality: even with careful planning, unexpected external and internal events can occur, causing predetermined initiatives or priorities to be deferred. Some feel that fire fighting is inevitable without a fully embedded and dynamic compliance culture. The question is how quickly you put the fires out.

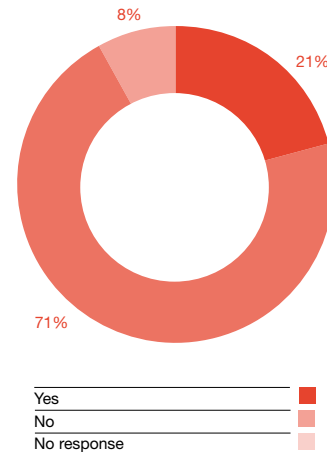
Sharing the load

The variety of activities undertaken by compliance officers and staff clearly demonstrates that the overall compliance effort is pervasive. As well as risk management, internal control and internal audit (whose collaboration with Compliance is discussed in more detail in the next section), respondents note that management, the legal department, HR, customer service/complaints handling, PR/external communications all have a role to play (see Figure 31).

Sixty-two percent of respondents say that management has a formal role. However, the perception of this role varies quite significantly, for example:

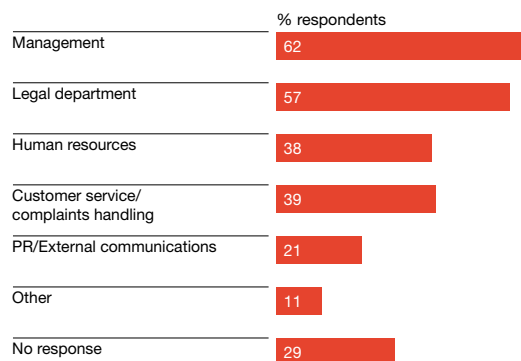
- Has ultimate responsibility for compliance/compliance plan
- Sets ethical standards and promotes values
- Supports through ‘tone at the top’ and information provision

Figure 30
Would you say the compliance function mainly operates in a ‘fire-fighting’ mode?



Source: PricewaterhouseCoopers

Figure 31
Which other parts of the organisation have a formal role to play in the compliance management programme?



Source: PricewaterhouseCoopers

- Provides first level of vigilance: oversight of compliance programme
- Has duty to oversee staff conduct in line with compliance policies and code of conduct
- Is involved in AML decision-making procedures
- Accompanies the project and provide guidance
- Identifies needs for specific compliance training
- Provides decisions on directives and procedures
- Chairs the compliance committee
- Proposes subjects to be assessed by the compliance function
- Monitors relevant compliance risks.

The perception of the legal department’s role also varied, for example:

- Keeps the compliance function abreast of new legislation
- Identifies issues that the compliance function should consider
- Provides counsel and advice on legislative interpretations

- Verifies legal framework and legal compliance
- Provides information and acts as a depository for legal framework in force
- Provides assistance in determining the impact of new legislation
- Advises on competition law
- Provides support, for example, with drafting compliance policies.

When it comes to the HR department, the percentage drops to 38%, but a variety of roles are highlighted (see Table 5).

Customer service and complaints-handling features in the compliance management programme for 39% of respondents.

Twenty-one percent see a formal role for public relations and external communications.

In addition, 11% of respondents feel other functions have a role to play. The composite list provides some insight into the different perceptions of the respondents:

- The business (as the first line of control)
- IT security
- Credit department
- Operations: payments filtering and second-line AML controls
- Back offices (transaction monitoring)
- Middle office
- Portfolio managers
- Supervisory board
- Investor relationship department
- External sales network department
- Project management department
- Capital investments department
- Marketing strategy department.

Table 5
Compliance-related responsibilities of other departments

<p>Human resources</p> <ul style="list-style-type: none"> • Information sharing on potential human risks in terms of fraud • Supportive, i.e. execution of decisions • Involved in the training process, including e-learning and identification of training needs • Cooperation with recruitment (measures to determine ‘fitness and properness’, where required) • Induction programmes for new joiners • Collecting signed staff confirmations of compliance with conduct of business rules • Filing documents related to employees and fulfilment of their duties • Ensuring the framework for the independence of compliance officers • Support with regards to compliance and integrity issues (integrity incidents, screening) • Disciplinary actions when needed • Setting procedures relating to conflicts of interest and confidentiality • Responsible for compliance with labour laws • Assistance with retention of compliance talent • Assistance with compilation of a skills inventory, mapped against compliance risks in the business • Assistance with establishing a skills development plan in line with future development strategy of the compliance function. 	<p>Customer service/complaints handling</p> <ul style="list-style-type: none"> • Information exchange • Reporting to all stakeholders, including Compliance • Record of all complaints • Evaluation of complaints • Ensuring that complaints are appropriately addressed • Escalating trends or complaints with significant impact (reputation risk) • Customer complaints communicated from the regulatory authorities • Apply standards and follow applicable complaints handling requirements • Front office and relationship managers complete client categorisation procedures, including all KYC/ALM documentation • Identify bad sales practices <p>PR/external communications</p> <ul style="list-style-type: none"> • Publication of disclaimers in client information • Cooperation in preparing defence against attacks on the firm’s reputation • Advice on communications with potential impact on reputation • Cooperation in mitigating reputation risk • All current and new regulatory and market developments • Apply required standards and promote the compliance culture • Assistance with public relations issues • Clear and legal marketing communications
---	--

The degree of integration of compliance risk management programmes

Clear trend towards a risk-based approach

An overall approach to compliance risk management should encompass risk identification, risk assessment, measures to manage risks actively and to mitigate them, as well as regular reporting (see Figure 32). The responses would indicate that, although the majority of respondents have taken all these steps into consideration, some – such as compliance risk mitigation – may not receive as much attention as other areas – or as much attention as they deserve.

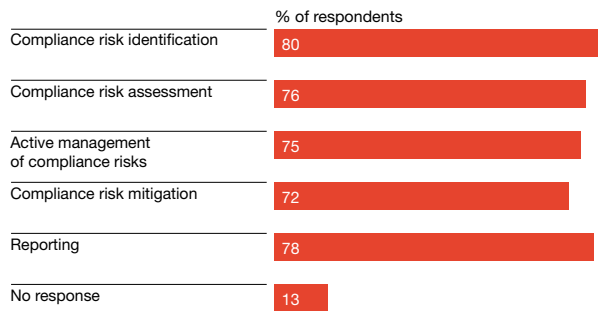
Where compliance functions are relatively new, the focus, not surprisingly, is more on risk identification and rectification, and on effective compliance risk management (see Figure 33). For longer established compliance functions, the emphasis shifts towards risk mitigation and management adopting a more holistic approach to embedding compliance into organisational structures and behaviours. Essentially, the approach needs to evolve, year on year. As one respondent stresses, a long-term, phased strategy to compliance risk management is necessary.

A clear majority of respondents have undertaken a risk mapping exercise to identify compliance risks to which their organisation is exposed. However, only 37% feel that compliance risk is well understood by business management within the context of all the risks to which the relevant business units/lines are exposed (42% feel the understanding is partial, and a further 14% that it is starting).

Forty-seven percent have adopted a risk-based approach to compliance risk assessment (with an additional 44% having done so partially, or starting to do so). This is perceived as an evolutionary process: first adopting a risk-based approach to compliance risk assessment and associated monitoring, then moving towards a more holistic risk-based approach to compliance risk management in line with a risk appetite approved by senior management and the board of directors. One respondent stresses that budget limitations often necessitate selectivity and prioritisation rather than the progressive drive towards efficiency. Only 25% have identified critical success factors for their compliance management programmes.

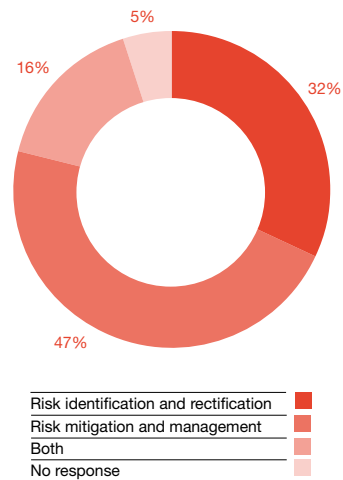
Nonetheless, 63% develop and fully document an annual compliance management plan/programme. Forty-one percent of respondents say this programme extends beyond the activities of the compliance function, focusing on enhancing compliance risk management throughout the organisation. Here again, with more recently established compliance functions, the

Figure 32
Does your overall compliance programme cover...?



Source: PricewaterhouseCoopers

Figure 33
Would you say your compliance management programme is geared primarily towards...?

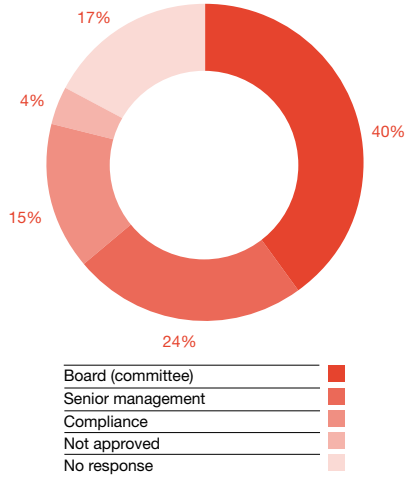


Source: PricewaterhouseCoopers

compliance management programme is more often restricted to specific, predetermined activities for the compliance function, rather than wider organisational efforts. The board approves the compliance work programme of 40% of respondents, and senior management 24% (see Figure 34 overleaf). Fifteen percent of respondents indicate that it is (group) Compliance that approves the programme, while 4% indicate that there is not, as yet, a formal approval process in place.

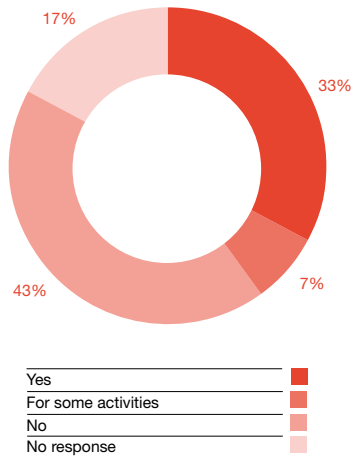
The concept of ‘competence centres’ applied to an overall compliance framework means an approach based on optimally exploiting key competences within other functions and departments. Thirty-three percent of respondents say that this

Figure 34
 Who approves the compliance management programme/plan?



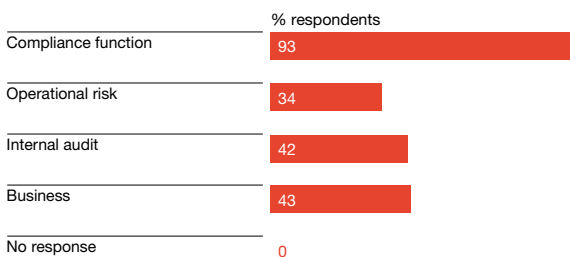
Source: PricewaterhouseCoopers

Figure 35
 Is the interaction between the different risk and control functions based on the concept of 'competence centres'?



Source: PricewaterhouseCoopers

Figure 36
 Who is responsible for identifying compliance risks within your organisation?



Source: PricewaterhouseCoopers

concept is applied within their organisation, and a further 7% that it is used in relation to certain activities – for example, anti-fraud, cyber risk, risk management tools, training and education (see Figure 35). Forty-three percent say it is not used formally, but some of these say they do use it informally or are moving, or intending to move, in this direction.

However, this may not always be, or be seen as, a predetermined tactic. Respondents indicate that involvement of other functions is necessary because of resource constraints. Also, individual members of the compliance function may, in fact, have other responsibilities (the most common combinations are Compliance with the legal department, or risk management responsibilities). So, differentiation between roles and responsibilities can be difficult.

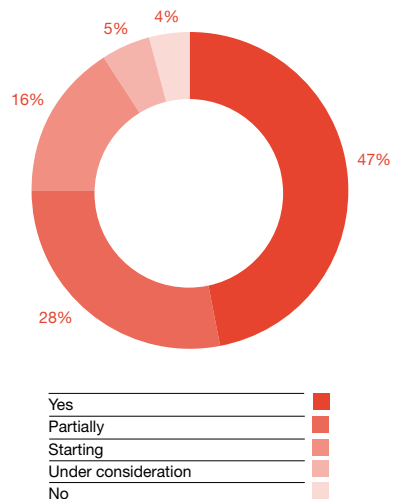
Risk identification

Ninety-three percent of respondents indicate that the compliance function is responsible for identifying compliance risks within the organisation (see Figure 36). A minority attribute (joint) responsibility to operational risk management, internal audit and the business. As mentioned above, the majority of respondents have developed risk maps or inventories identifying compliance risks relevant to different business lines, products or markets.

Risk assessment

In terms of compliance risk assessments (see Figure 37), 47% of respondents have adopted a risk-based approach; 28% have done so partially; and a further 21% (generally newly established compliance functions) are starting to adopt one or have it under consideration.

Figure 37
 Has your organisation adopted a risk-based approach to compliance risk assessment?



Source: PricewaterhouseCoopers

There are clear similarities in the risk assessment methodologies adopted by study participants. A common approach is first to undertake a comprehensive risk mapping exercise prior to assessing each identified risk in terms of its likelihood and the severity of the consequences of a compliance breach (financial, regulatory, operational, reputational, etc.). The positive effect of any mitigating measures in place is then taken into account (and scored), before prioritising the significant poorly mitigated residual risks for special attention. (It is worth noting that, in the majority of cases, 'compliance breach' for the purposes of the risk assessment relates to legislative or regulatory breaches.) Finally, an action plan is developed based on this assessment and validated by senior management and/or the board.

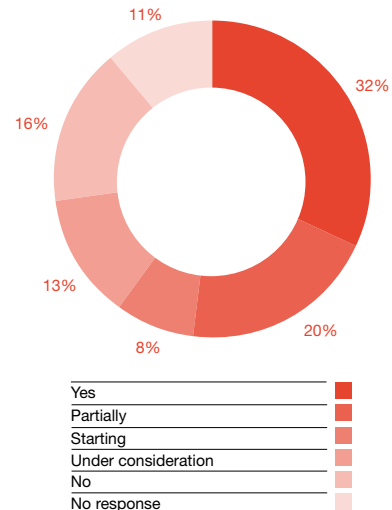
A number of respondents have been provided with risk assessment tools by their risk management department. However, some note that risk assessment tools developed by operational risk management do not necessarily adapt well to all compliance risks. One financial conglomerate notes that the compliance risk assessment methodology (and tools) mandated within the group as a whole was based on the banking business and was not expressly applicable to the insurance business. Others have, conversely, in the absence of an (operational) risk management tool, designed a purely compliance-driven risk assessment tool. One respondent comments that a tool developed by operational risk management could increase the level of 'professionalism' in the approach.

Only 14% of respondents note comparisons between the approach to compliance risk assessment and operational risk assessment under Basel II. Of these, the majority note similarities but also stress differences in the criteria used to score the risks, or say that the operational risk approach is more heavily geared towards analysing risk inherent in processes. In certain countries, respondents note that, because legal risk is included in operational risk under the Basel II framework, the same approach is adopted. One respondent has adopted a common group risk valuation matrix that encompasses internal audit, operational risk, Sarbanes-Oxley (SOX) and compliance risks.

The involvement of the business in the compliance risk assessment process is something the majority of participants have in common, often through a self-assessment process that is then used as the basis for ongoing, periodic reassessments and reporting. The format for the self-assessment is often defined by the compliance function following the initial compliance risk mapping exercise. Some respondents indicate that the overall assessment is undertaken on an ongoing basis by the compliance function. Few, however, indicate that the initial compliance risk mapping exercise is revisited on a frequent basis.

Potential regulatory or legal sanctions are often flagged as an important indicator for the compliance risk assessment. Interestingly, only 41% indicate that the costs of

Figure 38
Are key compliance risk indicators identified?



Source: PricewaterhouseCoopers

noncompliance are currently tracked. These costs include financial penalties, remediation costs, costs related to the suspension of business and business disruption, impact of cost of capital and impact on market share. Often, banks include relevant information in operational loss databases set up to comply with Basel II requirements. Other respondents indicate that tracking is done through incident reports and regular reports to management.

Marking a further refinement of assessment, 73% of respondents have identified compliance risk indicators (CRIs), are in the process of doing so, or are considering it (see Figure 38). To develop CRIs, some respondents divide compliance issues into specific fields with risky activities and/or processes given specific attention. CRIs are then derived from global policies or against certain themes (for example, reputation risk, AML risk, regulatory risk, financial risk) with specific risk events related to each theme. Others have developed CRIs in the context of a balanced scorecard that applies to all operations of their firm. Some note that information requests from regulators, material compliance breaches and/or customer complaints provided specific key CRIs. Many CRIs currently used are quantitative, for example (see Table 6 overleaf):

'Superficially considered as part of Risk Management but gets 'stuck' there....'

While some respondents note that CRIs may also focus on qualitative issues – such as reliability of internal controls or IT systems, level of automation, scope/type of new business or new markets, type and extent of training, and the types of complaint – the majority prefer quantitative CRIs at this stage.

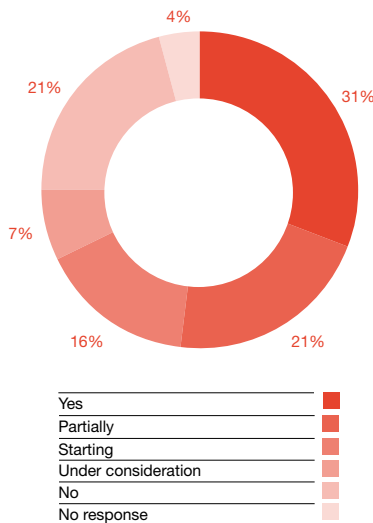
Table 6
 Examples of event driven compliance risk indicators

Number of full-time equivalents in compliance function	Number of requests from regulators
Number of training days (given and received)	Number of violations of compliance policies (by business line/unit)
Number and value of (potential) payout from lawsuits	Margin analysis
Number/financial impact of regulatory sanctions	Turnover ratio
Number/nature of client complaints (to the firm or to regulator)	Number (and type) of swap transactions
Number of compliance breaches	Number of new clients by profile
Number of employee complaints	Number of irregularities noted during client take-on Number/type of products and services
Use of internet by employees	Adherence to special dates regarding payments, transactions, products, customers, countries, procedures
Number of suspicious transaction reports (internal and external)	Number of employee declarations relating to gifts and invitations
Number of transactions made without authorisation	Number of disciplinary actions in relation to compliance breaches, including dismissals
Number of personal transactions by sensitive and non-sensitive personnel	
Number of declarations on insider dealing	

Establishing risk tolerance

Many respondents to our previous study suggest that senior management has expressed 'zero-tolerance' for compliance risks. However, this does not necessarily mesh well with a risk-based approach to compliance risk management. Asked whether senior management has determined the compliance risk tolerance underpinning a risk-based approach, only 31% say it has. Thirty-seven percent say that this has been partially done or is starting, and a further 7% that is under consideration (see Figure 39).

Figure 39
 Has senior management determined its risk appetite/tolerance in terms of compliance risk in line with a risk-based approach?



Source: PricewaterhouseCoopers

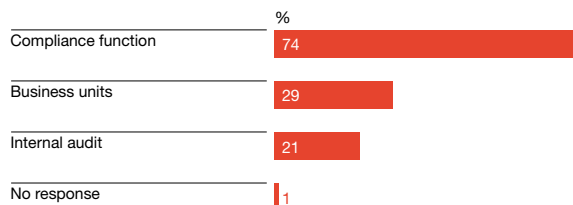
Risk monitoring and mitigation

Compliance risk monitoring

Seventy-four percent of respondents indicate that the compliance function is primarily responsible for compliance monitoring (see Figure 40). Twenty-one percent note a joint responsibility, generally with internal audit. Twenty-nine percent say primary responsibility lies with business units, and 20% with internal audit. Respondents note that when a compliance function has only recently been established, it needs to be involved widely and directly in terms of monitoring and control in order to identify gaps.

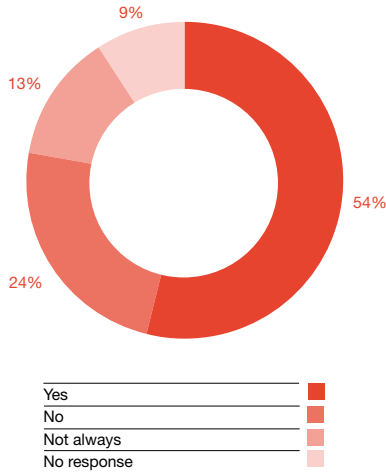
Asked whether the (group) compliance function undertakes regular monitoring of the activities of business units to ensure compliance with regulatory requirements, industry codes, best practices and internal policies, 37% say it does not, or not always (see Figure 41). Of the 54% who say that such regular monitoring occurs, the majority indicate that this is in respect of specific regulatory themes/ requirements, rather than broader compliance issues.

Figure 40
 Who is principally responsible for monitoring compliance?



Source: PricewaterhouseCoopers

Figure 41
Does the (group) compliance function undertake regular monitoring of the activities of business units to ensure compliance with regulatory requirements, industry codes, best practices and internal policies?



Source: PricewaterhouseCoopers

Notably, 55% also say that the compliance function has primary responsibility for ensuring that compliance monitoring is undertaken effectively (17% indicate that this responsibility lies with internal audit; 16% that it lies with the board, senior management or business management). This may suggest an inherent conflict of interest: where the compliance function not only monitors compliance but oversees that monitoring is carried out effectively. However, as one respondent notes, ‘monitoring’ is a much overused, and probably misunderstood, term, as it encompasses multiple responsibilities, including ongoing surveillance (for example, real-time transaction monitoring), oversight, follow-up, testing, etc. Clarity around what is actually meant by ‘monitoring’ in each circumstance is therefore important.

Only 32% of respondents say they use a formal methodology for compliance monitoring (the majority say an essentially risk-based approach has been developed at the group level). There are, however, common elements to monitoring programmes discussed by respondents. Once the compliance risk assessment is performed, gaps and weaknesses in the level of internal controls and findings from internal audit reports are taken into account when determining the compliance monitoring programme. Testing methodologies are established by type of risk, generally from a thematic perspective, with prescribed samples for each. Different types of risk, and different activities, require different testing approaches: from ongoing daily screening for suspicious transactions to staff and management interviews. Reflecting the perceived significance of the risks, respondents’ organisations allocate more resources to monitoring anti-money laundering and combating terrorist financing, investor protection, and the fight against market abuse and fraud, than for other compliance risks.

In terms of overseeing the effectiveness of the compliance monitoring programme, Compliance may receive regular reports from the business units (including self-assessments), organise frequent conference calls, conduct surveys and interviews with key stakeholders, and run workshops to evaluate whether monitoring routines are sufficient. One respondent says that each entity within its group submits an annual compliance monitoring programme, reflecting its specific activities, processes and resources, to the group compliance function and receives annual approval from senior management and the board before implementation. The (group) compliance function subsequently oversees compliance monitoring in line with the pre-approved monitoring plan.

Compliance risk mitigation

Monitoring is a form of compliance risk mitigation. In effect, a broad range of compliance function activities could also be regarded as risk mitigation. Firms are paying increased attention to various prevention measures that can also be described as forms of risk mitigation, such as broader compliance risk awareness raising initiatives or education and training.

For the purpose of this analysis, however, we focus on the responses in three areas:

- Effective internal control framework
- Breach and incident identification, escalation and reporting procedures
- Whistle-blowing programmes.

Internal control framework

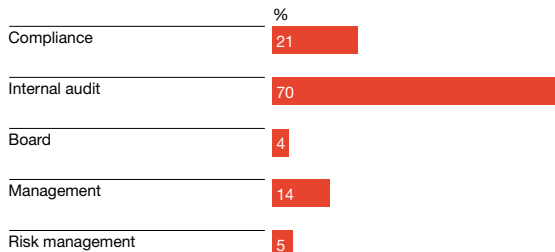
There are several aspects to an effective internal control framework, responsibility for which often lies with different functions, according to respondents:

- Identifying the risks, and conceptualising the appropriate controls
- Implementing, performing and overseeing compliance controls
- Evaluating and testing the effectiveness of the controls themselves.

Thirty-two percent indicate that the compliance function is responsible both for implementing compliance controls and for overseeing them. Again, although this may appear a conflict of interest, it is not necessarily, as the nature of the involvement may vary in each stage.

However, in terms of the internal control framework, only 14% say that they apply the ‘three lines of defence’, where risk management, internal control and internal audit all have a distinct role to play (see page 52).

Figure 42
Which function(s) are responsible for confirming the effectiveness of internal controls designed to ensure compliance?



Source: PricewaterhouseCoopers

The clear majority of respondents (70%) say the responsibility for confirming the effectiveness of internal controls lies with internal audit (see Figure 42). However, this is not an exclusive responsibility (it is often shared with the compliance function, business management, or occasionally risk management). Some respondents indicate that procedures and control points are developed at the group level and then rolled out, although there are questions about the effectiveness of this approach in dealing with local compliance risks.

An integrated firm-wide approach to internal controls – compliance and otherwise – is not widely adopted by respondents and less than half of respondents (46%) adopt a systematic approach to compliance controls. Where they do, the approach is often based – fully or partially – on Committee of Sponsoring Organizations of the Treadway Commission’s¹⁴ (COSO) approach, although, some respondents are not aware of the COSO framework. Some respondents have adopted a compliance risk and control framework based on Basel II principles or SOX 404, or a combination of the various frameworks. In-house assessment methodologies, on occasion, are adopted at the group level and rolled out.

Some approaches appear holistic. One respondent indicates that a control plan has been developed for each compliance domain for each entity, as well as an additional control plan for the ‘compliance framework’ that refers to the governance by, and overall organisation of, the compliance function. In this case, the control plans establish:

- Key requirements
- Description of implementing measures
- Owner
- Frequency of mitigating control
- Compliance self-assessment rating.

Breach and incident identification, escalation and reporting procedures

Sixty-four percent of respondents say there is a process established whereby breaches are reported to (senior) management. For 34%, serious breaches are reported to senior management and/or the board (or relevant committee) immediately

the facts are known, generally by the compliance officer and/or by the manager of the business unit where the breach has occurred. Subsequent, regular reporting to senior management and the board contains updates on breach resolution, as appropriate. In many of the newly established functions, escalation procedures are still under development. However, some respondents refer only to incident reporting as part of the periodic reporting to senior management or the board. Often, such reporting only takes place on an annual or semi-annual basis.

A number of respondents describe a combination of an established escalation procedure in line with (predetermined) levels of ‘materiality’ or ‘criticality’ (assessed by the compliance function), alongside regular incident reporting to senior management and the board. Some respondents mention a staged escalation process, where the severity of a breach determines how high within the organisation it is reported. In some cases, these processes were limited to more risky areas, such as AML, market manipulation and/or insider trading. Where the escalation process is based on materiality, it is not clear that all incidents are fully tracked and documented. However, the thorough documentation of incidents is seen as a key facet of the incident resolution process. Some respondents have developed standard incident reports; others rely on the details included in regular reporting or in a database and logbooks.

The process includes assessing what has happened, reporting the incident, and setting up measures to rectify or prevent recurrences in the future. One respondent mentions a quarterly follow-up procedure for corrective action that is designed to evaluate whether the remediation plan is being implemented properly.

Respondents mention various means by which breaches can be tracked:

- Reports by business (or by embedded compliance staff) to the compliance function when breaches are identified
- Compliance monitoring/testing can reveal further breaches
- Customer complaints
- Internal audit (or external audit) reviews
- IT systems (filtering and profiling) and internal controls.

Fifty-four percent say that root cause analysis is undertaken into identified breaches, although, in many cases, such analysis is restricted to material breaches. Once a breach is deemed to have been addressed, its cause is rarely revisited. Occasionally, root cause analysis is an explicit facet of a compliance management programme. A limited number of respondents have a database or dedicated tool for documenting all breaches (whether material or not) and their cause, their rectification, etc. Such systems can offer the possibility of a broader analysis that can look for any underlying patterns or correlations. Generally, however, respondents indicate that such analysis is not used to predict similar problems elsewhere in the organisation or behaviours that may lead to similar problems.

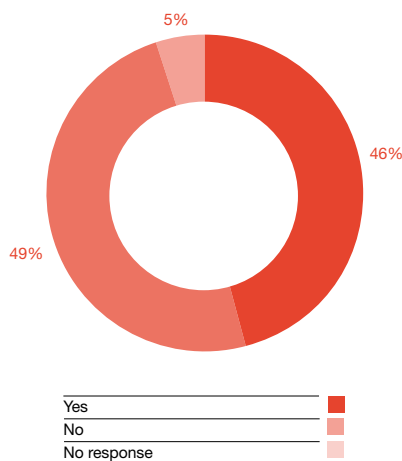
In terms of Compliance’s involvement in remediation, respondents mention:

- Assessment of incidents
- Involvement in disciplinary actions
- Determining corrective action and the introduction of additional controls
- Progress monitoring and reporting to senior management/board and group Compliance
- Feeding into ongoing risk mapping and assessments.

Whistle-blowing procedures

Some respondents feel that an obligation on staff to report all breaches or non-conformist behaviour, (for example, in branch networks, outsourced functions, etc.) is a useful supplement where incident-tracking procedures are under development. However, only 46% of respondents say that a whistle-blowing programme had been set up within their organisation, and for some this is a fairly recent development (see Figure 43). Even where whistle-blowing programmes have been in place for years, there had been limited use made of them. Some respondents feel this is due to cultural issues. Although not used widely in Western European countries, they appear to be used more frequently in Central and Eastern Europe (but with a significantly higher number of ‘false’ reports).

Figure 43
Does your organisation have a whistle-blowing programme?



Source: PricewaterhouseCoopers

Respondents’ programmes often encompass whistle-blowing policies made operational by anonymous toll-free telephone numbers, fax numbers or mail boxes. To preserve anonymity, some respondents indicate that reports are handled by independent parties within the group located outside the country where the alleged breach took place.

However, many respondents feel that the need for whistle-blowing programmes is replaced by an ‘open-door’ policy within the compliance function and employee confidence that any incidents reported will be handled confidentially and fairly.

Interaction with other risk and control functions

Forty-five percent of respondents say that other functions, such as risk management, internal control or internal audit, have day-to-day compliance responsibilities. Forty-seven percent, however, say this is the exclusive responsibility of the compliance function. Where collaboration or cooperation with risk management and internal control does occur, this relates principally to compliance risk identification, although the risk management function in a number of organisations also contributes to compliance risk assessments. Internal audit’s cooperation is also seen as having been primarily in relation to risk identification, although it too provides support in risk assessment, as well as compliance risk mitigation (see Figure 44). As MiFID specifies that the compliance function should fall within the scope of internal audit’s review remit, the opportunities for collaboration between the compliance function and internal audit are reduced, although not entirely removed.

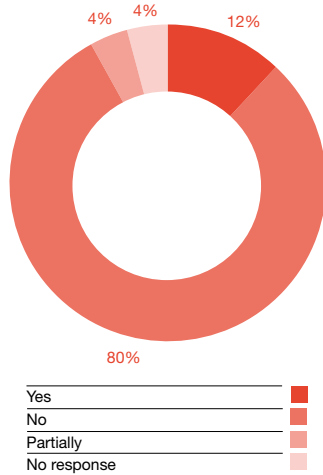
Figure 44
Involvement of other functions



Source: PricewaterhouseCoopers

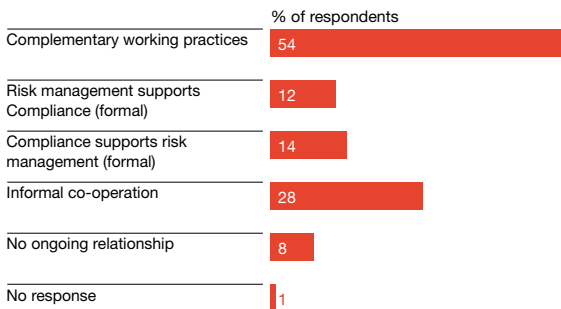
In smaller/less-complex organisations, cooperation between different functions can be achieved informally through operational committees comprising representatives of relevant functions (for example, compliance, risk management, internal control, legal department, human resources, complaints handling, internal audit, etc.). Thirty percent of respondents have operational compliance or coordination committees, bringing together representatives from these functions and, occasionally, other departments, such as client services, sales, HR and finance. Such committees generally work at the local or entity level.

Figure 45
Do you have SLAs in place between the compliance function and other risk control functions?



Source: PricewaterhouseCoopers

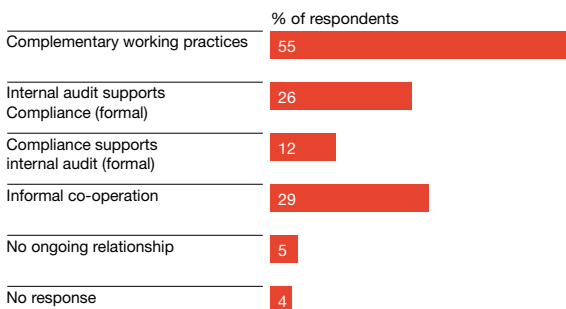
Figure 46
How would you describe the relationship between the compliance and risk management functions?



Multiple response possible: 1% of respondents did not respond

Source: PricewaterhouseCoopers

Figure 47
How would you describe the relationship between the compliance function and internal audit?



Multiple response possible: 4% of respondents did not respond

Source: PricewaterhouseCoopers

Compliance officers increasingly participate in, or have 'open invitations' to, risk management committees. Other committees to which compliance officers contribute include AML, new product/market, client acceptance, security, credit and investment committees.

Considering the nature of Compliance's interaction with risk management, internal control and internal audit, only 12% of respondents have formalised shared responsibilities by means of service level agreements (SLAs), while 4% have done so partially (see Figure 45). The majority of existing SLAs are with internal audit and/or internal control. Some respondents do not see the need for SLAs. They say that the responsibilities of various risk and control functions are clearly defined by their objectives or in charters, or that frequent meetings between them enable them to avoid misunderstandings or duplication.

In terms of working with the risk management function, 54% of respondents note that working practices are complementary. Twenty-eight percent say that the relationship is based on informal cooperation (see Figure 46).

Forty-three percent say the relationship with risk management has changed since our previous study. For 12%, these changes result from the establishment of either the compliance function or the risk management function, or through reorganisations. One Nordic respondent notes that the compliance function has been moved out of the legal department and into the risk management function. Another respondent notes that, where the compliance function was previously a subdivision of the risk management function, it has now been placed on an equal footing. For the remainder, the most prevalent change is enhanced cooperation between the two functions, often through parallel work on risk assessments. Some note, however, that the relationship has become more formal and contact is more regular than in the past.

Fifty-five percent indicate that 'complementary working practices' best describe the interaction with internal audit, while 29% say that the relationship is based on informal cooperation (see Figure 47). These results equate fairly closely with those above for risk management. This, combined with the fact that 26% of respondents indicate that internal audit formally supports the compliance function (compared with 12% that say the relationship is reversed), potentially raises questions on the independence of the internal audit function in certain organisations.

Half of the respondents do not perceive a change in the relationship between the compliance function and internal audit since our previous study. Thirty-six percent note a change that, in general, results from an evolution towards complementary working practices (beyond the informal cooperation of the past), improved information exchange and/or more formality in the relationship overall. Some attribute the latter to the fact that the compliance function is now a formal part of the scope of the internal audit, or to a clearer definition of roles (not least as

a result of regulatory provisions implementing MiFID). One respondent indicates that the relationship has improved because former auditors have moved to the compliance function, thus smoothing communication and cooperation between the two, as well as permitting the common use of audit and control tools. However, two respondents indicate that the relationship between the two functions has deteriorated over the past three years.

The extent to which the results of compliance risk assessments are shared with risk management and internal audit supports relatively close working relationships (see Figure 48). Sixty-eight percent share the results fairly extensively with risk management, while 70% share the results substantially with internal audit. The results of compliance monitoring are also shared with internal audit through the circulation of regular, formal reports. In organisations where the board committee responsible for compliance is also responsible for risk management and internal audit, result sharing is automatic. Otherwise, risk management receives the information through receiving reports formally or informally, through periodic coordination calls, breach notifications, or through meetings/discussions with the compliance function. One respondent mentions a database, accessible by all risk and control functions, which records issues identified.

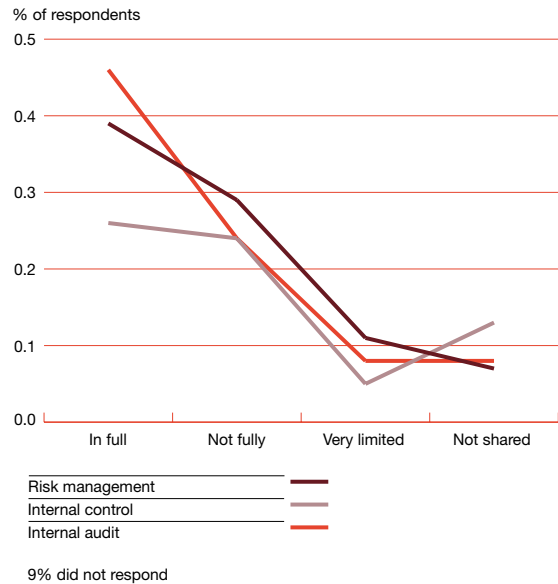
Three lines of defence

Internationally, over the past few years, the concept of the 'three lines' of defence has developed in relation to compliance risk management. This concept is based on i) frontline compliance monitoring undertaken, and controls performed, by the business unit; ii) oversight by the compliance function; and iii) ex-post review by internal audit. Forty-three percent of respondents say they apply, at least partially, this concept, most often in respect of AML requirements (see Figure 49).

In terms of its second line of defence role, oversight by the compliance function can be split into two main areas: i) ensuring that compliance monitoring is being carried out effectively; and ii) providing ongoing and broad-based advice to management and business. However, respondents provide the following examples of where the compliance function may act as, or supplement, the first line of defence monitoring activities (i.e. it is directly responsible for compliance monitoring):

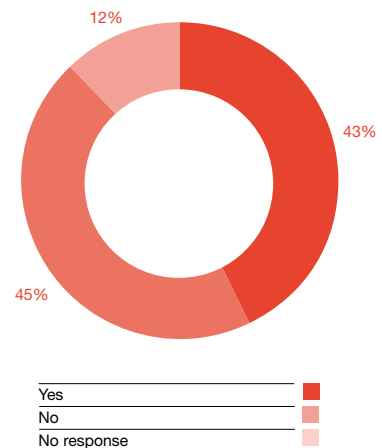
- Suspicious transaction monitoring and reporting
- Market abuse, insider trading and personal transactions
- High risk and politically exposed persons
- Investment restrictions
- Marketing communications with investors and clients
- Conflicts of interest
- Client acceptance/assessment procedures
- New business/operations
- Handling complaints received from the authorities
- Timeliness of reports to the regulatory authorities
- Outsourcing arrangements
- Internal conduct policy.

Figure 48
To what extent are the results of the compliance risk assessment shared?



Source: PricewaterhouseCoopers

Figure 49
Do you apply the concept of the 'three lines of defence' to compliance monitoring?



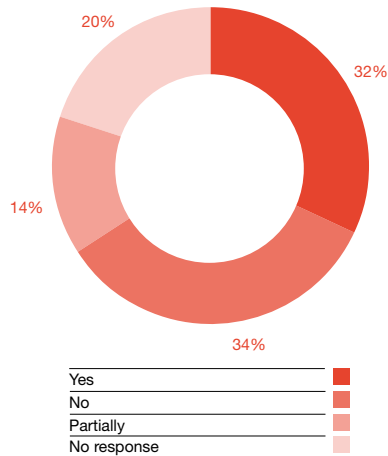
Source: PricewaterhouseCoopers

A number of respondents emphasise that differentiating between the lines of defence was a considerable challenge. One notes that it is not possible to move to a 'three lines of defence' approach rapidly, saying this needs to be done progressively and systematically, clarifying roles and responsibilities in each area over time.

Second line of defence: advising the business

A number of issues relating to effective compliance monitoring and overseeing it are discussed earlier in this report. The study suggests that many respondents still face limited understanding of the breadth of their role. Asked whether the difference between the compliance management programme and the compliance monitoring plan is well understood within the organisation, 48% feel that the difference is not or is only partially understood (see Figure 50). Some believe that such understanding is deficient even at senior management level.

Figure 50
 Is the difference between the compliance management and the compliance monitoring programmes well understood within your organisation?



Source: PricewaterhouseCoopers

A number of respondents hold polarised views of the role. While some believe that the compliance function's role encompasses only compliance monitoring, others see monitoring as just part of the function's mandate. This, essentially, represents the difference between the roles of 'policeman' versus 'counsellor' – concepts based on the existing preconceptions within the organisation. For those subject to MiFID, the extension of the role of either 'policeman' or 'advisor' is seen as having increased the potential confusion within the business.

Senior management of 64% of respondents requires compliance officers to sign off new products, sometimes with the right of veto and some respondents are involved in client acceptance procedures. Five percent of respondents participate in management or other committees and are aware of any plans. However, the majority receive the information after the event (for example, receiving relevant committee minutes

and periodic reports, from intranet sites or via networking with business units, risk management and internal audit). Only one respondent notes that it is the responsibility of the business to inform the compliance function of all new developments, while another says that there is no intervention by the compliance function except on the demand of the business. One respondent notes that while involvement of the compliance function in the new product/activity approval process is mandatory, its advice is not always respected, and another says that the business does not accept this intuitively as part of the compliance function's remit. There are, therefore, questions about form over substance.

Respondents are less involved in decisions relating to technology enhancements for business purposes, although the compliance function may verify ex post that new systems are able to ensure compliance. The need to involve the compliance function early in decisions on systems with an express compliance dimension (for example, to meet MiFID best execution requirements or privacy and data protection rules) is more readily accepted. That said, there is a sense that, over the past three years, additional attention has been paid to compliance by IT (security) departments with these functions, rather than the compliance function being involved in such deliberations.

'Talk, talk, discuss, train, train, talk, assess, report, talk....'

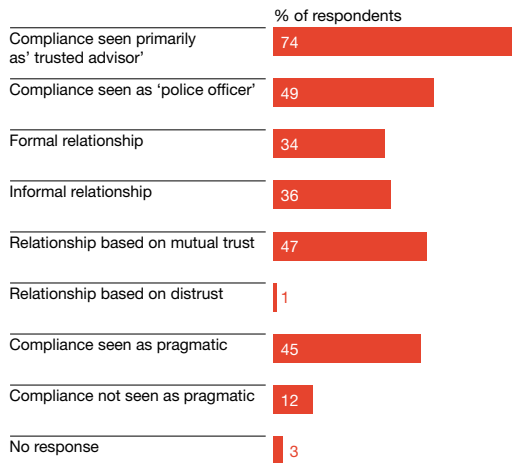
Most respondents' activities are geared towards enhancing the understanding of compliance processes throughout the organisation. This was done through training, compliance risk self-assessments, control activities (including explaining to managers and staff the reasons why things went wrong), ongoing advice around transactions and activities, and reporting. One respondent stresses the benefits of linking all staff evaluations (and remuneration) to their demonstrable compliance with relevant rules. Another says that employees are required to pass a 'compliance skill review' every two years to ensure compliance with both external and internal rules. However, these respondents are in the minority.

Seventy-four percent of respondents believe that the compliance function is perceived as a trusted advisor by management and the business. Only 49% say that Compliance is perceived as a 'police officer' (see Figure 51), supporting the view that Compliance's advisory role is seen as taking precedence. However, only 47% also feel that the relationship is built on mutual trust, and only 45% that Compliance is seen as pragmatic. One respondent stresses that the key is to 'anchor [compliance risk management processes] well with management and ensure communication with employees'.

However, questions remain about the nature of this communication and who is responsible for it, and also about the credibility of the compliance function.

Figure 51

How would you describe the interaction of the compliance function with front-end business(es)?



Multiple responses possible

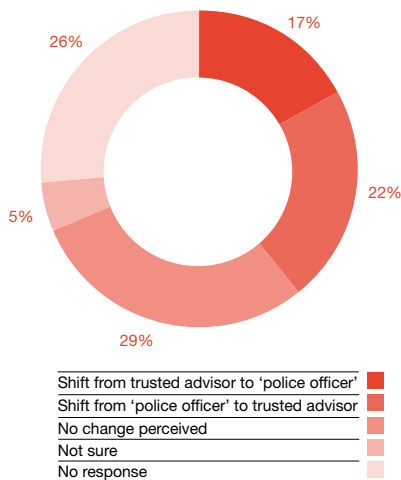
Source: PricewaterhouseCoopers

Overall effectiveness of the compliance function

Only 25% of respondents have developed a broad-based approach to assessing the effectiveness of the compliance function. The lack of a clear methodology is considered the main hurdle.

Respondents feel defining a methodology is difficult due to the potentially polarised roles of the ‘counsellor’ and ‘police officer’. Our previous study stressed the need to balance the two roles. This study found no definitive shift in either direction (see Figure 52), although respondents note that specific legislation can push the pendulum in different directions (for example, AML rules place more emphasis on the ‘police officer’). Consequently, one assessment methodology may not be suitable for all aspects of the compliance function’s work.

Figure 52
 Have you experienced a shift in either direction?



Source: PricewaterhouseCoopers

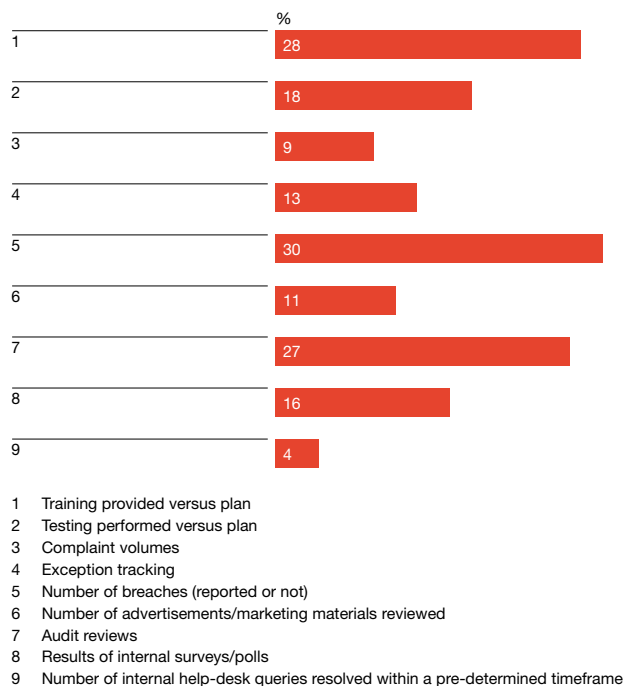
In terms of the shift, Scandinavian and Belgian respondents have seen an increased emphasis on the ‘police officer’, with some suggesting that the pendulum has swung too far at times. Larger organisations in other countries note a similar trend. The majority of respondents feel that the advisory role needs to be primary, because being seen primarily as a control function jeopardises its ability to influence business decisions effectively. As advisors, they feel that Compliance is better placed to help management both embed a compliance culture and navigate the future complexities of more ‘principles-based’ regulation. Newly established compliance functions, though, need time to establish their credibility as trusted advisors. Respondents note that, assessing the quality and consistency of advice, and the value that it brings to the business, is challenging.

A common message from respondents is that new legislation, particularly MiFID, has increased the workload of the compliance function substantially. On the positive side, respondents believe that MiFID has clarified Compliance’s role and enhanced its profile within the organisation. This has led to strengthened international coordination within the function, and increased trust in the business but also increases expectations.

Effectiveness assessments

Some of the fundamental bases for effectiveness assessments are not yet in place. In the first instance, the assessment of compliance function effectiveness is generally left to periodic internal audit reviews, but only 24% of respondents say a detailed assessment of the effectiveness of compliance function processes has been undertaken as part of that review. Again, only 24% indicate that compliance function processes have been evaluated according to their completeness, timeliness, consistency and sophistication.

Figure 53
 On what issues do KPIs generally focus?



Multiple responses possible

Source: PricewaterhouseCoopers

Key performance indicators

In general, where annual compliance management plans are in place, respondents say that effectiveness assessments were undertaken and reported against these plans. However, this is not always on the basis of pre-established key performance indicators (KPIs). Only 33% have identified KPIs for the compliance function, but these are often limited in scope. One respondent notes that KPIs have been established for reporting at the central/group compliance level but not for monitoring, advisory and training. He expects that establishing KPIs may be simpler at the local entity level. Only 17% of respondents link compliance personnel objectives to KPIs identified for the compliance function as a whole.

Where KPIs have been identified, these often focus on quantitative measures (see Table 7). However, quantitative measures, while useful for CRIs to inform monitoring plans, are not necessarily appropriate performance measures, and they need to be seen in context. An increase in the number of breaches could, for example, suggest that the compliance function has improved its detection methods or that compliance within the business is deteriorating. In terms of its performance, the compliance function will always face the challenge of proving a negative – for example, a reduction in the number of breaches that might otherwise occur.

That said, more established compliance functions are looking to improve effectiveness assessments by using more qualitative KPIs, for example:

- Management and employee satisfaction surveys
- Subjective and informal assessments by the board and/or senior management
- Reviews by group Compliance
- Quality of reporting and internal communications
- Quality of compliance training

- Quality of external communications
- Quality of relationship with the regulators
- Customer satisfaction surveys
- Performance against compliance objectives included in employees' personal objectives (e.g. as part of a balanced scorecard)
- Peer reviews and benchmarking
- Speed of progress in reducing and mitigating compliance risk
- Quality and consistency of solutions found to remedy problems
- Speed in rectifying compliance breaches and/or weaknesses
- Effective roll-out of new compliance initiatives, particularly large compliance projects
- Timely completion of action plans
- Extent and quality of external networking (e.g. with industry associations).

Respondents suggest that some negative measures, such as the avoidance of negative media coverage, major incidents, and regulatory sanctions and assessments of reputational damage caused by compliance breaches, cannot be avoided altogether for the purposes of the assessment but need to be seen in context.

Some respondents use dashboards to help monitor performance – in general on the basis of quantitative KPIs. Qualitative KPIs could form part of regular reporting, sometimes subject to control by group Compliance. One respondent notes that this latter process culminates in review sessions, scoring and relative quality assessments.

In the main, the respondents note that assessment of the performance of the compliance function is more closely aligned to the results and effectiveness of compliance monitoring than to the performance of the compliance function overall.

Table 7
Quantitative KPIs

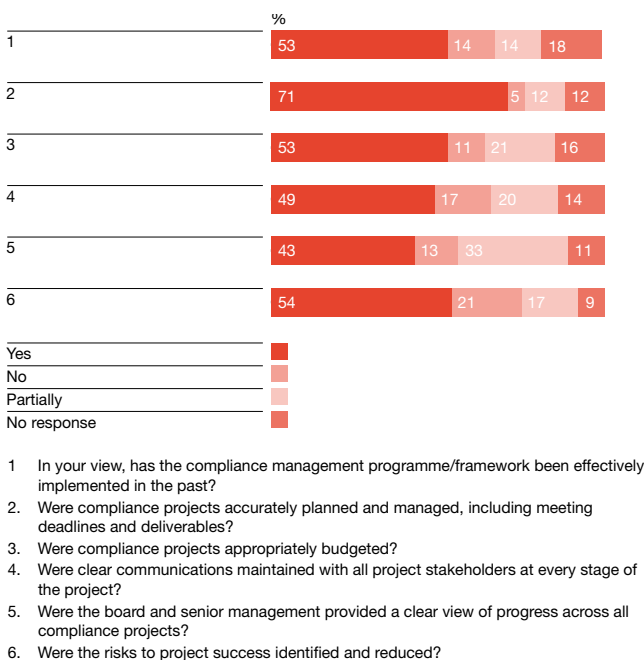
- | | |
|---|--|
| <ul style="list-style-type: none"> • Resolve backlog • Number of compliance findings as a result of monitoring • Number and status of compliance recommendations • Number of breaches • Number of AML/CTF suspicious cases – transactions investigated within a predetermined timeframe • Number of preliminary evaluations of new structures, processes, contracts submitted by the holding company or legal entities • Number of staff • Number of full-time equivalents in the compliance function versus number of training days given or received • Number of helpdesk enquiries • Measurement of cost in respect of each major piece of legislation (e.g. the cost of Basel II or MiFID implementation) | <ul style="list-style-type: none"> • Number of investigations/queries of regulatory authorities • Number of new regulations with relevance to Compliance • Number of suspicious transactions investigated • Number of new products/activities reviewed before launch • Participation in committees (new products, new projects, credit committee, client acceptance committee, audit committee) • Number of policies and procedures developed/rolled-out • Number/type of meetings with regulators • Complaints per product/campaign • Complaints frequency/volume • Number of internal helpdesk queries resolved within a predetermined timeframe |
|---|--|

Performance to date

Asked about performance to date, the majority of respondents (54%) consider that their compliance management programmes have been implemented effectively. However, these programmes are not often comprehensive. As seen earlier, these programmes evolve, focusing first on specific regulatory requirements, such as suspicious transactions reporting, before expanding towards a more holistic approach. The longest established comprehensive programme appears to be just 4 years old; others are in a 'testing' phase. In response to the question, 'Has the compliance programme/framework been effectively implemented in the past?', one respondent says it has been implemented 'as effectively as possible, taking into account our means, manpower, reporting lines and management support'.

Asked if mechanisms have been put in place to assess the resilience of the compliance framework overall, 28% of respondents indicate that they have been. However, even among some of the more established respondents, such initiatives are deemed premature or a 'work-in-progress'. One respondent indicates that group Compliance has identified special interest topics on which it wants a consolidated view, and requires quarterly reports. Others have set up focus groups; undertaken internal benchmarking, to look for examples of good practice within the group as a whole that might be leveraged more widely; and undertaken extensive policy, product, process, contract and communication reviews (including mystery shopping, product reviews, etc.), using stress tests.

Figure 54
 Were compliance projects managed effectively?



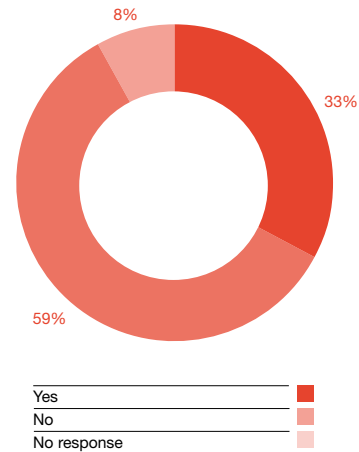
'No response' includes 'not relevant'

Source: PricewaterhouseCoopers

Effective project management

In terms of specific compliance-related projects, many respondents indicate that their firm's approach is often 'reactionary' when dealing with new regulatory requirements. Forty-three percent say that compliance projects are accurately planned and managed, including meeting deadlines and deliverables, while 53% feel that risks to project success are identified, but not necessarily appropriately mitigated (see Figure 55). Fifty-one percent say the approach adopted for compliance-driven projects does not differ from the approach for business processes.

Figure 55
 Has a plan been developed to assess and improve the processes used by the compliance function?



Source: PricewaterhouseCoopers

In terms of project success, respondents note that project plans can be disrupted by external factors beyond the organisation's control. One Greek respondent recalls that strikes in the Greek banking sector delayed its AML/CFT implementation project. Other respondents note that missed deadlines and deliverable requirements are often due to the 'intrusion' of day-to-day responsibilities and/or unrealistic deadlines. For one respondent, a project delay resulted from changes to current procedures and systems (including new software implementation) that were not adequately taken into account in project planning. Another notes that delays also occur as a result of inadequate cooperation with other units. One notes that there is a learning process for the compliance function with regard to rolling out compliance projects across the organisation and this can impact overall effectiveness of related projects.

While 49% say that compliance projects are properly budgeted, others feel that budgets are often insufficient or that the budgeting process proves problematic as 'indirect' costs are not factored in. For example, costs 'buried' in business line budgets or human resource and technology costs, are not adequately foreseen.

The responses show different approaches to allocating responsibility for compliance-related projects. In some cases, there is a graduated approach: major implementation projects, such as MiFID implementation, are owned by senior management; less complex projects are owned by the business. Compliance's involvement ranges from being the project driver to the overseer. In quite a number of cases, however, the compliance function is seen as responsible for all compliance-related projects.

Seventy-one percent of respondents say that senior management is provided with a clear view of progress across all compliance projects. Fifty-three percent say that all project stakeholders are kept informed throughout the life of the project – for example, through regular (steering committee) meetings or conference calls with affected departments. Respondents note that communication is key when managing stakeholder expectations, but also that communications can always be improved. However, for some, the only feedback provided to the board or senior management in terms of project progress is as part of regulator reporting, sometimes only on an annual basis.

Improving compliance processes

The lack of focus on compliance function processes implied above is relatively systematic. Only 33% of respondents have developed a plan to assess and improve selected compliance function processes (see Figure 56), with 26% reviewing such plans on an annual basis. Respondents say that improvements are assessed, inter alia, on overall efficiency, level of 'client' satisfaction and effectiveness of risk mitigation. While many perceive that assessment and improvement is a continuous focus, only two indicate that this is part of an organisation-wide initiative to improve processes on an ongoing basis. One respondent mentions that, as part of the integration process following a merger, compliance function methods are being compared with a view to harmonising and improving these processes, while simultaneously establishing best practice.

Figure 56
What use does the compliance function make of technology?



Source: PricewaterhouseCoopers

Thirty percent of respondents have plans in place to assess and improve compliance weaknesses and deficiencies in all key business processes; 8% plan a partial review. Responsibility for monitoring progress falls generally to the compliance function, sometimes in conjunction with senior management and/or internal audit (36% of cases).

In terms of specific processes, respondents' approaches to KYC and conflicts of interest are discussed earlier in this report (see page 23 and 24).

Process improvements

Sixty-four percent of respondents integrate their approach to market abuse with personal transaction monitoring, so far as possible, when considering potential market abuse by staff. Others are working on this. Market abuse by clients, or the measures to prevent traders accessing sensitive information, is generally handled separately. There are questions as to whether and how monitoring should be done 'real-time'. One respondent notes that the value of ex post compliance reviews – in terms of personal transactions of senior management or board members, who may have mandates in several companies group-wide – is questionable. Generally, respondents have established (group-wide) policies that clarify the principles for personal transactions – for example, in terms of:

- Status of the person (sensitive, regular insider, occasional insider, people having access to estimated results)
- Scope of prohibited transactions
- What are the obligations linked to this status
- What is privileged information
- Reporting requirements to the regulatory body
- Definition of blackout periods.

Other processes that respondents have addressed as a result of MiFID or the Insurance Mediation Directive include:

- Administration of financial instruments
- Procedures concerning investment research
- Inducements
- Best execution
- Sale of third-party products
- Client categorisation (and assessment)
- Valuation of assets in respect of unlisted companies
- Gift and entertaining policy
- Whistleblower policy
- Outsourcing
- Record keeping
- Automation of insurance mediation processes.

Some respondents have appointed MiFID compliance officers or established specific control programmes around MiFID compliance.

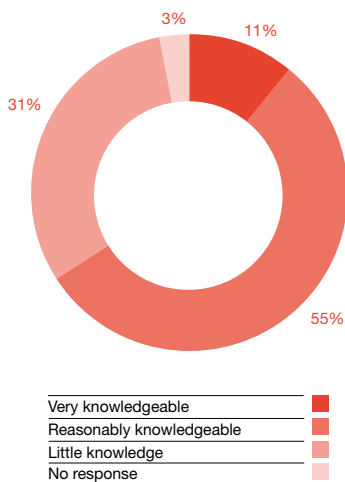
'... without the full collaboration of IT nothing is possible.'

Use of technology

Most respondents indicate that Compliance uses technology primarily to monitor specific activities. For example, 82% use it to monitor and report suspicious transactions; 71% to monitor KYC requirements; and 59% to monitor personal account dealing (see Figure 57). Twenty-four percent have developed dashboards to facilitate reporting. Other uses of technology mentioned include:

- AML controls
- Incident management
- Breach reporting
- Transaction reporting
- Sanctions screening
- Customer complaints
- Scrutiny of fund managers and custodians
- E-learning.

Figure 57
 Are members of the compliance function aware of all the technologies and systems used within the organisation?



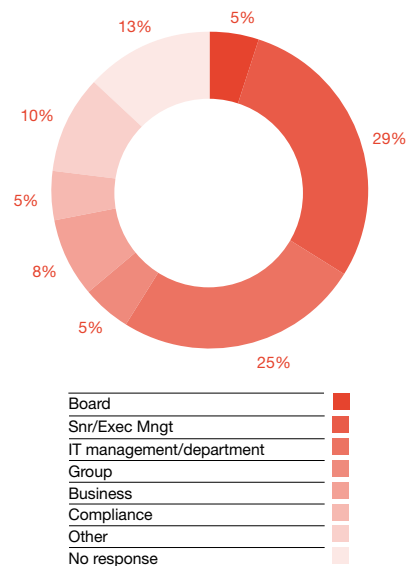
Source: PricewaterhouseCoopers

Respondents keep up to date with compliance technologies available in the marketplace by talking to their peers and external consultants, attending seminars and workshops, research on the internet and in relevant publications, and through dialogue with technology providers of all kinds. Some respondents also note that industry associations' working groups were often helpful in this respect. For some, the IT department is the 'go to' group for such information. Others mention IT specialists, within or aligned to the compliance function, who provided support in researching new technologies.

Sixty-six percent of respondents believe that members of the compliance function are very, or reasonably, knowledgeable about the technologies and systems (including legacy systems) used by the organisation (see Figure 58). Forty-seven percent believe that the IT department is very, or reasonably, knowledgeable about compliance requirements and issues. Many IT departments are responsible for IT security policy and procedures, now working closely with the compliance function. Asked what role the IT department plays in the compliance management/monitoring programme, responses range from 'a big role' to 'no role'. The IT department is seen as a system provider, an application and tool developer, as well as a support mechanism providing reports and analysis at the request of the compliance function or in the event of major projects. However, where IT is an outsourced function, the compliance function receives limited support in this area.

Thirty-six percent of respondents say that priority is given to compliance-related developments by the IT department when there is a legislative imperative (50% say no priority is given). Fifty-nine percent say the board and senior management at group or business level determine the priorities for the IT developments for compliance. Ten percent say that the compliance function itself determines the priorities (see Figure 58).

Figure 58
 Who determines the priorities for the IT department in relation to compliance tool developments?



Source: PricewaterhouseCoopers

Effective communications with the compliance function

In terms of communication within the compliance function, where the compliance function is newly established and still small, sharing results of compliance monitoring and other compliance activities is not a major challenge. For other respondents, information is in general shared through a combination of: compliance and other committee meetings, compliance function meetings and 'away-days'; systematic communication and compliance alerts; personal visits; on-the-job training; and regular reporting, conference calls and feedback within the compliance function.

Only 11% specifically use technology to facilitate communication within the compliance function and compliance function activities (for example, permitting direct access to compliance monitoring tools, and shared drives or libraries).

Contacts

Pan-Europe

Ullrich Hartmann

Tel: +49 69 9585 2266

Email: ullrich.hartmann@de.pwc.com

Wendy Reed

Tel: +32 2 710 7245

Email: wendy.reed@pwc.be

Austria

Andrea Cerne-Stark

Tel: +43 1 501 88 1720

Email: andrea.cerne-stark@at.pwc.com

Doris Wohlschägl

Tel : +43 699 111 61908

Email: doris.wohlschlaegl@at.pwc.com

Belgium

Denis Caprasse

Tel: +32 2 710 7216

Email: denis.caprasse@pwc.be

Czech Republic

Jiri Klumpar

Tel: +420 251 152 077

Email: jiri.klumpar@cz.pwc.com

Denmark

Henrik Axelsen

Tel: +45 3945 9980

Email: hax@pwc.dk

Germany

Ullrich Hartmann

Tel: +49 69 9585 2266

Email: ullrich.hartmann@de.pwc.com

Martina Rangol

Tel: +49 69 9585 2280

Email: martina.rangol@de.pwc.com

Greece

Kyriakos Andreou

Tel: +30 210 6874680

Email: kyriakos.andreou@gr.pwc.com

Ireland

Garvan O'Neill

Tel: +353 1 792 6218

Email: garvan.o'neill@ie.pwc.com

Italy

Fabiano Quadrelli

Tel: +39 02 6672 0538

Email: fabiano.quadrelli@it.pwc.com

Mauro Panebianco

Tel: +39 02.66720568

Email: mauro.panebianco@it.pwc.com

Michele Cancelliere

Tel: +39 02.66720216

Email: michele.cancelliere@it.pwc.com

Luxembourg

Emmanuelle Henniaux

Tel: +352 49 48 48 21 11

Email: Emmanuelle.henniaux@lu.pwc.com

Netherlands

Martin Eleveld

Tel: +31 20 568 4317

Email: martin.eleveld@nl.pwc.com

Poland

Adam Wnek

Tel: +48 22 523 4735

Email: adam.wnek@pl.pwc.com

Romania

Dan Iancu

Tel: +40 21 202 8500

Email: dan.iancu@ro.pwc.com

Slovakia

Silvia Marusincova

Tel: +421 903 781 615

Email: silvia.marusincova@sk.pwc.com

Spain

Francisco Velasco

Tel: +34 91 5684327

Email: francisco.velasco.correa@es.pwc.com

Antonio Carrascosa

Tel: +34 91 5684634

Email: antonio.carrascosa.morales@es.pwc.com

Borja Guisasola

Tel: +34 915 68 4937

Email: borja.guisasola.marrodan@es.pwc.com

Sweden

André Wallenberg

Tel: + 46 8 555 341 62

Email: andre.wallenberg@se.pwc.com

Åsa Malmström Rognes

Tel: +46 8 555 33 633

Email: asa.malmstroem.rognes@se.pwc.com

Switzerland

Christiana Suhr Brunner

Tel: +41 79 223 5010

Email: christiana.suhr.brunner@ch.pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

PricewaterhouseCoopers provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

'PricewaterhouseCoopers' refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, the PricewaterhouseCoopers global network or other member firms the network, each of which is a separate and independent legal entity.

For further information about this report, please contact Ullrich Hartmann, PricewaterhouseCoopers Financial Services Central Cluster Regulatory Leader, on +49 511 5357 5709 or at ullrich.hartmann@de.pwc.com or contact Wendy Reed, Director, PricewaterhouseCoopers Risk Assurance Services, on +32 2 710 7245 or at wendy.reed@pwc.be.

Designed by studioec4 19882 (11/09)

pwc.com

© 2009 PricewaterhouseCoopers. All rights reserved. 'PricewaterhouseCoopers' refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.



Printed on paper manufactured in the EU containing both recycled and virgin fibre from sustainable sources.