The Future of Compliance

Compliance functions as strategic partners in the new regulatory world

kpmg.co.uk
CONTENTS
“Firms need to adapt to a new regulatory framework while dealing simultaneously with a vast range of other national and international regulatory reforms.”
INTRODUCTION
The global regulatory landscape is currently undergoing a fundamental change. In response to the recent financial crisis, regulators across the globe are focusing on a programme of more robust supervision of financial services firms whilst also introducing a raft of new regulatory initiatives to bolster the regulatory framework.

Changes in the UK regulatory architecture, with the moves towards ‘twin peak’ regulation and the Financial Services Authority (FSA) committing to a more intensive and intrusive supervisory approach focusing on both prudential and conduct risk, show that profound changes to the regulation of the global financial services industry are unlikely to let up any time soon.

A strong focus on improving transparency in markets and products, providing greater investor and consumer protection are central to the substantial new regulation and updates to existing rules that are bearing down on the industry.

In the UK, firms need to adapt to a new regulatory framework while dealing simultaneously with a vast range of other national and international regulatory reforms: Basel 3’s higher capital and liquidity standards (for banks and investment firms), Solvency II reforms (for insurance companies), recovery and resolution plans, the final recommendations of the UK’s Independent Commission on Banking and additional requirements being discussed for systemically important financial institutions (SIFIs), among many others.

Recent experience has shown that even those firms that appeared well capitalised and risk aware have been subject to regulatory censure. No firm is exempt from the need for constant change and renewal. Failure to adapt to the changing regulatory requirements could have serious impacts for firms, both in their relationship with the regulator and potential sanctions imposed by the regulator.

Amid expectations of greater transparency of board-level compliance reporting and pressures on the board to ‘own’ compliance, more needs to be done to position the function as an integral and strategic element of business.
THE FINANCIAL CRISIS HAS TESTED THE RESILIENCE OF SOME OF OUR MOST TRUSTED FINANCIAL INSTITUTIONS. CONSUMERS’ TRUST IN THESE INSTITUTIONS HAS ALSO BEEN TESTED BY, AMONGST MANY THINGS, THE FACT THAT PRODUCTS HAVE BEEN DESIGNED IN WAYS THAT DID NOT MEET THEIR NEEDS, AND SOME SALES PROCESSES HAVE PUT THE PROFIT OF THE FIRM AHEAD OF THE BENEFITS FOR ITS CUSTOMERS.

Martin Wheatley, FSA MD and CEO designate of the FCA, July 2012

How regulated firms (re-)structure their Compliance functions to respond to, or preferably pre-empt, these complex challenges will encompass the range of culture, strategy and people. Not only the function’s composition, but also its role and voice within the business and overall risk management framework, should be considered.

Although it is difficult to quantify the value added by Compliance, fines and censure can highlight the potential cost of non-compliance. The number of regulatory disciplinary cases initiated by the FSA has increased over recent years – 66% in 2011 v 58% in 2010. In 2010/11 the FSA also issued a record level of fines - £98.5m. Over more recent months, substantial fines have also been levied by the FSA on firms for large-scale failures in controls and oversight. These statistics point towards increased regulatory expectations on firms.

An effective Compliance function is key to identifying and mitigating risk and protecting the business from regulatory censure and protecting brand and reputation.

Leading firms will see these external changes as an opportunity to enhance the value-adding aspects of Compliance. Seeing the potential, but also recognising the limitations, in their Compliance functions will help them in the pursuit of growth as well as dealing with threats, creating competitive advantage and improving corporate value and reputation in line with growing stakeholder demands around integrity, accountability and financial stability.

We believe that there has rarely been a more opportune time for firms to rethink or build upon their compliance approach, assessing whether it is fit for purpose in the new regulatory environment and whether it will remain so in light of developments looming over the horizon.

Drawing on research, insights and experiences of working with financial institutions to explore the current and potential impacts of their Compliance functions, this report suggests ways in which firms might engage with emerging issues in order to ensure that their Compliance expertly and safely guides them through turbulent times.

Having reviewed current and impending changes to the UK regulatory framework, we provide an assessment of how we believe these changes will in practice impact the role and nature of Compliance within regulated firms.

Regulatory and Compliance arrangements are driven by the impact of regulation on the organisation and their risk appetite. The precise design of a compliance framework will therefore vary for individual firms. While there is no ‘one size fits all’ solution, our analysis focuses on the core considerations in how a Compliance framework may need to change in order to cope with regulatory change:

- Risk Management Framework
- Role of Compliance within the business
- Compliance structure
- Compliance strategy
- Compliance monitoring
- Compliance Management Information
- Resourcing
- Interaction with regulators

© 2012 KPMG LLP, a UK limited liability partnership, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.
RISK MANAGEMENT FRAMEWORK

The FSA has been active in voicing its concern that Compliance functions should be independent from the business to ensure their effectiveness as risk management and corporate governance tools. In addition, firms are under pressure from the regulator to ensure that Compliance is a standing agenda item for senior management and the board to enable proactive management of regulatory risks – the criticism sometimes levelled being that regulatory compliance is a secondary concern for senior executives.

In analysing firms’ risk management frameworks we considered in particular the impact of regulatory change on:

- The structure of each organisation’s risk management framework, including whether or not they adopt the FSA’s traditional ‘3-Lines of Defence’ model, and where Compliance sits within the framework of each organisation
- The ownership of risk within the business
- Risk governance structures, including reporting lines for Compliance and where regulatory compliance risks and issues are considered within each business.
RISK MANAGEMENT FRAMEWORK

The FSA is already applying greater scrutiny to firms’ risk management frameworks. This is evident from the FSA’s supervisory framework (new ARROW) approach and it is likely to be a continued area of scrutiny for both the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) following the transition to twin peak regulation in 2013, although each entity will engage with the issue from different perspectives.

In our experience, the vast majority of UK financial services firms employ the traditional ‘3-Lines of Defence’ model, with clear demarcations between each line in the management of risk:

First line: Business line management
Second line: Risk and Compliance functions
Third line: Internal Audit

Issues with these models tend to be around unclear or ill-defined spans of control and responsibilities between the lines of defence. In order that the risk management framework may operate effectively, it is vital for each element within the framework to have a clear understanding of its role, the risks it is tasked with managing, the tools at its disposal and how these can be deployed. The board and senior management team have a key role to play in setting the framework for their business and assigning responsibilities.

While we believe the 3-Lines of Defence model will continue to be the most appropriate model to allow firms to adequately identify, manage, and mitigate the risks to which they are exposed, firms must take a more holistic view of their risk management framework in order to ensure that all risks to which their business is exposed are captured. Firms will also need to understand where there are ‘touch points’ within the model, for example where a change in the risk profile of one part of the business will impact on other business areas.

The increasing weight of new regulatory legislation from the European Commission, coupled with the increasingly diverse and complex risks to which firms are exposed, means that firms need to ensure that no risks fall between the cracks.

Undertaking annual exercises such as a Risk Inventory Assessment would provide comfort to both the board and FSA that the business has identified all the risks to which it is exposed and is able to map those risks to where and how within the business they are managed and monitored. Firms that are able to demonstrate evidence of such risk mapping should ensure that they are on the front foot with the regulator.

OWNERSHIP OF RISK

Following the fallout of the recent financial crisis and criticism from the FSA that risk was not a sufficiently prominent feature of boardroom discussions, a clear expectation of the FSA is that Risk and Compliance is now owned by the board, with due attention on board agendas.

Current supervisory framework visits have reinforced this expectation. FSA investigations regarding governance require clear evidence of the extent to which the board has not only assumed ownership for Risk and Compliance but also actively considers matters such as risk appetite, risk profiles, and challenges risk and compliance management information.

In demonstrating ownership of risk within the business, the regulator expects boards to:

Set the tone from the top
Discuss and establish risk appetite
Monitor key business risks and the business’s performance against risk appetite.

Key to this is the setting of ‘tone’ from the top of the business, as the FSA identified a primary contributor to the recent financial crisis as being the lack of a compliance culture within firms. Consequently, assessment of a firm’s compliance culture is attaining prominence in the FSAs supervisory approach. Supervisory framework reviews are interviewing a broader spectrum of individuals than previously, although the focus remains on senior management, interviews are being increasingly conducted across and down through the business. This is set to continue with the FCA’s forward-looking, judgment-based approach to supervision.

In order to establish a truly compliant culture, boards need to drive evaluation of culture on an ongoing basis.

There does not necessarily need to be a single common mechanism by which boards exercise ownership of risk. Oversight may be delegated to a board sub-committee such as a Risk Committee. Ultimate responsibility must not be delegated, however, and clear defined reporting lines must exist for the escalation of key issues.

A board’s ability to oversee and manage regulatory compliance can only be as good as the information it receives. Involved parties therefore need to know which regulatory compliance matters are reserved for the board if a compliant culture is to be effected.

KEY QUESTIONS TO CONSIDER

Do you have accountability for Risk and Compliance running throughout the organisation, and how do you ensure this?
Do you have a clear structure of ‘risk owners’ within the business?
FIRMS NEED TO TAKE RESPONSIBILITY FOR THE WAY THEY TREAT THEIR CUSTOMERS AND MAKE SURE THAT GOOD CONSUMER OUTCOMES ARE EMBEDDED THROUGHOUT THEIR BUSINESS MODELS.

Martin Wheatley, FSA MD and CEO designate of the FCA, July 2012
Depending on the size and scale of the business, a number of committees may be needed in order to consider the disparate exposures and risks.

The committee(s) should report to a board sub-committee that is similarly responsible for the oversight and management of regulatory compliance risks, and ultimately up to the Board.

Such a clearly defined risk governance structure provides evidence of strong ownership and accountability for compliance throughout the organisation.

**KEY QUESTIONS TO CONSIDER**

- **Does your governance structure evidence strong ownership and accountability for compliance within the business?**
- **How many and what composition of committees are required to effectively handle the range and extent of risks and exposures the scale of your business generates?**
The Future of Compliance

 ROLE OF COMPLIANCE

Firms need to have a clear vision concerning the role of Compliance. The debate can often be whether it should act in an advisory capacity supporting first line business management in discharging the firm’s regulatory obligations or whether it should have an oversight and enforcement role in monitoring business activities. In practice, future developments in the regulation space are most likely to require a combination of the two.

With an overarching goal of helping to guide organisations through regulatory changes and safeguarding them from the far-reaching implications of non-compliance (including but not limited to financial and reputational consequences), its role must evolve in line with regulators’ expectations and the emergence of new obligations.

In the context of the Compliance function’s role, we sought to analyse the impact of regulatory change on:

The vision of Compliance within the business, including responsibilities and its operational mandate

Management of regulatory compliance risks within the business.
The Future of Compliance

VISION OF COMPLIANCE
At the highest level, the strategic vision of Compliance should be defined and set by the board in formal terms of reference.

Broadly speaking, the role of Compliance should be to take the lead in identifying and managing the significant regulatory compliance risks to which the business is exposed, including:

- Designing and supporting a regulatory risk framework for the business
- Supporting and challenging business line management regarding the completeness and accuracy of compliance risk management activities, including identification and measurement
- Providing advice to business units on regulatory obligations and on the creation and implementation of regulatory compliant policies and procedures
- Monitoring the organisation’s compliance with relevant laws, regulations and internal risk policies
- Reporting on compliance matters that warrant the attention of senior executives.

KEY QUESTIONS TO CONSIDER
Do you have a formally stated, clearly articulated vision for Compliance?
Has the board approved the strategy for Compliance to meet its objectives?
Does the business have clear mechanisms for measuring the performance of Compliance against strategy?

PRAGMATISM SHOULD PREVAIL
In considering the future role of Compliance, firms must determine whether Compliance should act as a review, oversight and monitoring body, independent from the first line or whether it should act as a partner to the first line, being a guide and sounding-board to help prevent regulatory breaches from occurring.

The debate must also take into account the function’s level of independence: while distance from the first line enhances objectivity and independence of oversight and monitoring, a closer working relationship with the business allows greater direct involvement in avoiding regulatory problems.

The stated objective of the FCA to take a more “forward-looking, proactive, judgment-based (approach to) supervision...crystallis(ing) the change from the old style reactive approach to the new style proactive approach” would imply that there is a strong case for Compliance functions to act as a partner to the business in explaining the regulatory responsibilities of the business, helping to frame regulatory compliance policies and acting as a guide to help prevent regulatory breaches from occurring within the business. The recent fall-out from Payment Protection Insurance (PPI) and pension mis-selling makes a strong case for more direct involvement of Compliance in the business.

Financial institutions will increasingly rely on Compliance functions to help them interpret and apply new legislation arising from the European Commission. However, to ensure compliance, the monitoring role remains key.

To get the balance right, therefore, pragmatism may dictate a combination of guidance and monitoring activities, whereby Compliance takes both an advisory and monitoring role:

Advisory: to partner with the business and provide guidance on the interpretation of regulatory requirements, and delivery of operations in line with the firm’s regulatory risk appetite

Monitoring: to undertake independent compliance monitoring of the business against the firm’s regulatory risk appetite.

To retain the independence of each of these activities, however, it is important that these activities are undertaken by separate teams within the Compliance function.

Horizon scanning is a further, crucial area of responsibility for Compliance, particularly so in a fast-moving regulatory environment. Timely identification of legislation that will have a direct or indirect impact on the business is vital, with subsequent escalation to senior executives, assessment of the likely impact on the business and its risk profile, and of course designing the firm’s response.

Only a minority of firms currently set an explicit expectation that Compliance should actively review upstream risks and assess the impact of ongoing regulatory developments.
The Future of Compliance

WE WANT FIRMS TO HAVE A CULTURE WHICH ENCOURAGES INDIVIDUALS TO MAKE THE APPROPRIATE JUDGMENTS AND DELIVER THE OUTCOMES WE ARE SEEKING. AT ALL TIMES WE WANT AN INSTITUTION TO ACT WITH INTEGRITY.

Hector Sants, FSA CEO, October 2010
Currently within both retail banking and insurance, responsibility for the identification, assessment and measurement of regulatory risks rests with Compliance in around half of organisations, while in the other half it lies with line management, supported and challenged by Compliance.

In all cases, Compliance is involved in identifying and assessing regulatory risks in each business line, whether directly or through providing assistance, support and challenge to line management.

The board should review, challenge and ultimately sign-off on regulatory risk assessments. This evidences good governance, oversight and the active involvement of senior management.

In order to comply with expected European Commission legislation, we expect this risk assessment and understanding of regulatory risk profile to be an annual exercise.

The majority of financial services firms currently involve the board via board sub-committees (risk and/or audit committees) in the oversight and governance of regulatory risks identified by the business. What will be important in the future is the extent to which the committees understand their role in ensuring a sound regulatory control environment and in challenging senior management.

**KEY QUESTIONS TO CONSIDER**

- Are responsibilities for identifying regulatory risks within the business clearly allocated?
- How do you ensure regulatory risks are adequately identified? Does Compliance have a prominent role?
- Are committee responsibilities for the oversight of regulatory risks clearly defined?
- Are there any potential areas of overlap or a danger that risks may fall between the cracks?
A viable and effective Compliance strategy should be driven by the business’s regulatory risk profile and the risk appetite set by the board, ensuring an appropriate Compliance role, adequately resourced and directed in enabling the business to manage and mitigate its regulatory risks.

**WE WILL HAVE A GREATER EXPECTATION OF A STRATEGIC APPROACH TO THE CONDUCT AGENDA AND SENIOR MANAGEMENT AND BOARD ENGAGEMENT IN IT.**

Clive Adamson, Director of Supervision, Conduct Business Unit, FSA, January 2012
In addition, recent FSA supervisory activity has shown a distinct expectation of the board’s involvement in developing and approving the Compliance strategy, thereby helping the board to discharge its responsibility to oversee and manage the risk profile of the business.

In analysing the Compliance strategies employed by firms reviewed, we have sought to understand the impact of regulatory change on the following elements:

Formulation and communication of risk policies
Development of an overarching Compliance strategy for the business.

TAILORED RISK POLICIES
As the regulatory environment evolves, the development and maintenance of risk policies becomes increasingly important. A formal process for policy design and approval will enable firms to put in place policies that are robust and appropriate, whilst on-going monitoring and maintenance will facilitate them remaining appropriate.

Risk policies should reflect the regulatory environment of the individual firm, mitigating the regulatory risks to which it is exposed through its operations.

Firms that recognise the link between regulatory risk assessment and the development of risk policies may better tailor policies to specific risks.

With increasing expectations from the regulator that senior executives will be involved in the oversight of regulatory compliance matters, a process for senior management approval for all risk policies is essential.

Risk policies of the majority of financial services firms with which we have worked are currently designed at group level by a Group Risk Committee. This risk function typically owns the risk policy, being responsible for identifying risk and reviewing risk assessments carried out by individual business segments.

Responsibility within a small number of organisations is held at board Risk Committee level, while an even smaller proportion delegate it to individual business segments.

In the vast majority of firms, risk policies are ultimately approved by the board through its Risk Committee.

KEY QUESTIONS TO CONSIDER

Does your business have a clear and effective structure and process for the design and approval of risk and compliance policies?

Is there also a clear and regular process for the on-going monitoring of risk policies to ensure that they remain appropriate and robust?

COMPLIANCE STRATEGY
2011 was a year of substantial change and forward planning across regulatory systems and approaches and in the nature, scope and reach of the overall regulatory environment.

From a strategy perspective, the role of a financial institution’s Compliance function needs first and foremost to be mindful of the four pillars around regulatory change:

1 Prudential implications:
   - Determining who is accountable for what in terms of the prudential side of, inter-alia, planning asset and cash management and liquidity management
   - Understanding what challenges the regulator is likely to set in terms of the amounts of capital firms must hold – in both Pillar 1 and Pillar 2.

2 Firms’ approaches to:
   - Governance and decision-making
   - Planning and strategic execution.

3 Understanding the customer agenda:
   - In terms of customer coveners, which flows in terms of Europe from PRIIPS, the IMD, MiFID 2 and other regulations likely to concern relevant products such as mortgages. The focus is generally on customer engagement and is increasingly on firms ‘getting it right’ with minimal adjustment where necessary - failure to do so invites considerable pressure from the applicable regulatory body, raising questions about strategic decision-making.

4 Firms’ control infrastructures, comprising:
   - Internal infrastructure: internal systems and controls
   - External infrastructure – external / third-party systems such as BACS and BCP exchanges. Firms will be required to demonstrate and evidence how external systems are engaged as part of business-as-usual and how they are integrated and managed accordingly.

Compliance plays a critical role in all of these considerations.

CUSTOMER-CENTRICITY
Of particular concern to firms will be the regulator’s renewed focus on the customer agenda, especially with the FCA’s remit to ensure fair customer outcomes and protecting and enhancing the integrity of the financial system.

Press coverage over PPI mis-selling has demonstrated the cost of getting compliance wrong in the customer sphere. As the eye of the FCA becomes increasingly trained on the way in which firms interact with customers, firms need to recognise the role of Compliance in monitoring interactions with customers; also to ensure this role is built into the Compliance charter and strategy.

Far from being a ‘tick the box’ function, Compliance is key to protecting brand values and reputations in managing the way the business interacts with customers – from the perspectives of advisory (developing risk policies and procedures, etc.) and oversight (monitoring and upward reporting).

It is therefore essential that firms have a clear idea of the role of the Compliance function in customer interaction, that this is clearly articulated and understood throughout the business, and that Compliance is equipped with the necessary tools to meet these expectations.

We observe in most cases that firms have a compliance strategy in place, in which the board is involved and approves via its Risk Committee. Such strategies are typically in place either via a charter or a mandate and, in some cases, as part of the annual compliance plan.

KEY QUESTIONS TO CONSIDER

Does your business have a clear Compliance strategy with a robust, proactive mechanism for ensuring that applicable regulatory change is implemented and embedded in a timely manner?

Does your Compliance function have a prominent and defined role in overseeing customer interaction to ensure that good customer outcomes are achieved?
Compliance function structures have come into greater focus over recent years, tending to adhere to either a centralised or decentralised model, the choice of which is dictated largely by the extent of the organisation’s global presence and diversity of its business operations.

In analysing the structure of Compliance within firms reviewed we have sought to understand the impact of regulatory change on the following elements:

- Whether organisations employ a centralised or decentralised Compliance structure
- Compliance presence within divisions and reporting by divisional teams to Group Compliance
- Interaction between Group Compliance and divisional Compliance teams.
WHAT WE HAVE LEARNT FROM THE PAST IS THAT THINGS GO WRONG WHEN BUSINESS MODELS ARE NOT BASED ON A SOUND FOUNDATION OF FAIR TREATMENT OF CONSUMERS, AND A STRONG CULTURE THAT SUPPORTS THIS, LEADING TO PRODUCTS BEING SOLD THAT ARE NOT SUITABLE FOR THOSE BUYING THEM.

Clive Adamson, Director of Supervision, Conduct Business Unit, FSA, June 2012
FIRMS SHOULD ENSURE THAT THEIR SYSTEMS AND CONTROLS, INCLUDING COMPETENCE OF EMPLOYEES, KEEP PACE WITH ANY CHANGES IN THEIR STRATEGY AND BUSINESS MODEL, AND WITH ANY NEW SERVICES THE FIRM IS OFFERING.

MONITORING

Compliance monitoring is central to providing assurance to senior management that the business is adequately managing its regulatory risk exposure and that the controls and policies in place to manage these risks are effective. The recent financial crisis has led to a growing appreciation of regulatory risk as a key component of a business’s overall risk profile. A clearly defined programme of risk monitoring is vital and without this, the identification of risks, which is a core element in risk management, means little.
Indeed, a key requirement of the FSA’s ‘SYSC’ rules is that Compliance monitors and assesses the adequacy and effectiveness of the risk management measures in place. Some tensions may arise, however, between Compliance’s roles in providing advice and guidance to the business and that of performance monitoring. In this respect, it is important that firms are able to demonstrate that monitoring is independent.

Reporting of compliance monitoring activity is also an important consideration, especially how and to whom results are reported. The FSA’s expectation is that monitoring activity will be reported in some format to the board, however the content and format of this reporting varies between firms. In analysing the activity of compliance monitoring within firms reviewed, we have sought to understand the impact of regulatory change on:

The design and direction of compliance monitoring activity

Reporting of compliance monitoring results.

DESIGN AND DIRECTION

The Compliance function has traditionally been concerned primarily with advice and monitoring around conduct. This raises the question how it ensures a compliance culture is embedded within a firm, in turn ensuring the constituent parts of the business are joined-up. This is set to grow as a challenge and compliance monitoring must come to terms with the ‘new normal’ of tougher, more aggressive supervision. Partly as a result, firms are expressing concern over booming legal and non-legal compliance costs.

The fact that cultural change is embedded in the firm must be clearly demonstrated. Looking at the change process relating to regulatory change around for instance RRP if the business is not fully engaged, it will fail to be fully effective. There is thus a need for an understanding of the change process throughout the business.

A further major issue that firms must consider is how to determine the firm’s compliance universe:

What does it look like in its entirety?

How are monitoring accountabilities and responsibilities allocated through the business (e.g. clear demarcations between Compliance and Internal Audit responsibilities)?

How does the firm define qualitative and quantitative measures to provide assurance that applicable compliance risks are being captured and monitored? Some responsibility may lie with the Compliance department, some on other parts of the business such as Operations Risk.

How does it all fit together – who will be the ‘ring-master’, ensuring that when people need to be engaged, they fully understand the agenda?

Compliance monitoring must get tougher if it is to meet the challenges and adequately cover the areas in which the FSA will show greater interest, such as:

Product governance

Outsourcing (particularly data security risk and business continuity on termination of a contract)

Deep dives into client assets and the new realm of suitability and appropriateness (i.e. looking not just from a sales advice perspective, but earlier in the process from development, target markets and distribution channels)

Where the compliance monitoring function sits within an organisation (should it be an advisory or a monitoring department or both)?

Is monitoring akin to audit or day-to-day oversight?

Which elements of the Compliance function sit within the Compliance department and which within the business?

In terms of the direction of compliance monitoring, how is the related information collated, irrespective of where it sits, both in terms of responsibility and accountability?

Formally approved compliance monitoring plans are a must, as are the right resources in terms of quantity and quality to deliver the plan. Beyond this, it is the risk appetite statement and the tolerance levels underpinning it, as set by the board, that drives compliance. Well articulated statements and tolerance levels provide a clear view regarding the level of risk a company is willing to take, consequently setting Compliance a clearer remit when performing its monitoring activities.

REPORTING OF MONITORING RESULTS

Given the FSA’s increased focus on the involvement of senior management in the oversight of regulatory compliance, it is imperative that firms build a clear reporting structure into compliance monitoring plans in order that instances of non-compliance can be escalated to senior management once they are identified.

While the exact nature of this reporting can be established according to each firm’s specific needs, as a minimum Compliance functions should report instances of non-compliance via the Risk & Compliance Committee, Executive Committee and, subsequently, the Board Risk Committee or Board Audit Committee. This reporting mechanism allows senior management teams to be aware of instances of non-compliance as they occur and to assess the potential impact on the firm.

KEY QUESTIONS TO CONSIDER

Do you have a risk-based compliance monitoring plan in place to guide compliance monitoring activity within the firm?

Is this plan subject to regular review to ensure that it remains appropriate for the risk profile of the business?
RESOURCING

FSA rules require firms to ensure that the Compliance function has the necessary resources to undertake its responsibilities and to provide relevant assurance to the business. Indeed, quality and quantity of resourcing is a critical success factor for any Compliance function to fulfil its responsibilities within the agreed risk appetite.

Profit and capital protection has recently been behind a freeze on hiring and discretionary spend within many financial institutions. However, evolving UK regulation requires firms to invest in their control and assurance functions, not least Compliance. As a result, firms are attempting to strike a balance between reducing overheads and maintaining a robust and effective Compliance function.
This inherent tension can best be summarised by a consideration of:

**Costs of compliance, including staff salaries, benefits and training as well as space and associated technology costs; versus**

**Costs of non-compliance, including financial penalties, remediation costs, suspension of business/business disruption, impacts on cost of capital and market share.**

Given the FCA has been clear that supervision will be more intrusive and they will be making pre-emptive judgments on products and circumstances deemed unsuitable, it is increasingly vital that Compliance functions employ experienced Compliance Officers who are able to challenge the business prior to the FCA seeing a need to.

In analysing firms’ current arrangements we have sought to understand the impact of regulatory change on:

- The number of FTEs within Compliance functions
- Responsibility for resourcing and remuneration of Compliance.

**RESOURCING**

Despite the greater supervisory challenge expected from the FCA, a knee-jerk reaction of increasing Compliance resourcing may not necessarily be right. Firms should instead spend the meantime re-evaluating the role of Compliance and ensuring that its remit is well articulated and embedded within the business. Only when such decisions have been made by the board can firms turn their attention to required resourcing levels. Throwing resources at the problem will not fix it if the framework itself is broken.

An important area for firms to consider their Compliance resourcing is in the split between their advisory and monitoring teams. As discussed earlier in this report, an effective Compliance function must strike the right balance between advice and monitoring.

Ensuring the correct split of resources between these two teams will permit more rigorous testing and additional reviews to be undertaken to provide assurance to stakeholders (backward-looking – ‘reactive’) and to ensure potential issues are dealt with proactively (forward looking – ‘pro-active’).

Although Compliance teams may not necessarily need expanding even given the new regulatory supervisory approach, they will need to ensure they have sufficient experienced Compliance officers with the right mix of skills to cope with new regulatory initiatives (e.g. Solvency II, RDR etc) and who are capable of challenging the business effectively.

From our work in the industry we have found that there is no optimum Compliance resourcing model. Risk and Compliance resources are, instead, largely dictated by the size of a business and the regulatory risks it faces:

- **Size of the business**
  - Nature of the products sold by the business
  - Wider risk management structure
  - Nature of the distribution network.

Our review of current arrangements shows that the majority of organisations in the retail banking sector employ 51 to 100 FTEs in their Risk and Compliance functions. The largest resource pool identified was in excess of 500 FTEs. Of those retail banks analysed that have a wide global presence, 60 percent had more than 200 FTEs within their Risk & Compliance functions.

**RETAIL BANKS**

Responsibility for ensuring adequate and appropriate resourcing of the Compliance function should lie with the Head of Compliance. Emerging UK and European regulations re-shaping the market will affect banks, insurers, investment firms and corporates.

The skills profile of a well designed Compliance function should be tailored into the regulatory initiatives on the horizon with which Compliance will have to deal. If Compliance functions fail to retain the right skill sets they will not be able to provide the advice required by the business. The Head of Compliance must ensure that their team has the right skill set mix to be able to deliver a holistic approach to these inter-connected regulations.

Equally, the Head of Compliance must be able to recruit the right people that set the tone and culture to enable them to lead their part of the business.

Regulatory risk should be afforded as much importance as credit or market risk and, as such, the Board Risk Committee and senior management must be satisfied that it is adequately resourced. We would expect the Head of Compliance to present at least annually to senior management on resourcing matters. In this respect we would also expect to see resourcing overseen by formal committees at either executive or board level.

**KEY QUESTIONS TO CONSIDER**

- **Is your Risk & Compliance function sufficiently robust to challenge the business effectively?**
- **Have you recently revisited your Compliance resourcing model? Do you feel you have sufficient coverage to manage the regulatory risks to which you are exposed, as well as increased regulatory supervision?**

**SETTING COMPLIANCE REMUNERATION**

The Head of Compliance should be responsible for setting the responsibilities of Compliance Officers, thereby protecting the Compliance function’s independence by ensuring that first line senior management does not dictate the remit of Compliance.

As regulatory risk should be afforded the same importance as credit or market risk, we would expect remuneration of the Head of Compliance to be reviewed and set by one of the Audit Committee, Risk or Remuneration board sub-committees and to be in line with other department heads.

Having a board sub-committee be responsible for remuneration helps to maintain Compliance’s independence from business line management.

Increasingly, firms include Compliance soft metrics in a balanced scorecard to appraise and evaluate business line management. This move towards compliance-based remuneration is an effort to embed a compliant culture within firms. Given the increased emphasis on regulatory compliance within firms and the increasingly intensive and intrusive supervisory approach of the regulator in the UK, we would expect to see an increase in this measurement of compliance culture and behaviours in remuneration.

**KEY QUESTIONS TO CONSIDER**

- **Have you considered the ‘compliance’ impact on remuneration within your business?**
- **Are employees appraised using a balance scorecard which includes ‘compliance’ metrics?**
Much criticism has been levelled at financial institutions following the financial crisis to the effect that Compliance information was of insufficient detail and not escalated to senior management when appropriate.

The regulator’s expectation of Compliance Management Information (MI) broadly extends to ensuring that firms have in place a reporting framework that seeks to ensure the proper and effective reporting of key regulatory risks and issues, with escalation to the appropriate board committee.
In analysing the nature of Compliance MI within firms reviewed we have sought to understand the impact of regulatory change on:

- Where and to whom Compliance MI is reported
- The content of Compliance MI
- How senior management is appraised of regulatory compliance risks and any identified material breaches of FSA rules.

EXECUTIVE LEVEL REPORTING

The sign of an effective Compliance culture is not necessarily the structure in place but the quality of Compliance MI generated and reported upwards. If the MI quality is poor or is not reported through the appropriate channels, senior management cannot have a clear understanding of how well the organisation manages its regulatory risks.

All organisations should operate a reporting mechanism for Compliance MI to executive level committees, which should be either Executive Risk Committees or dedicated Compliance Committees, ensuring the information reaches the appropriate audience.

Where necessary, Compliance MI should be escalated to more than one of the Executive Committee and other executive level committees such as the Risk Committee and Operational Risk Committee.

The format and content of Compliance MI provided to executive level committees should focus on demonstrating the effectiveness of established processes in order to ensure the business's compliance with relevant laws and regulations.

Compliance MI should encompass consolidated Compliance reports from individual business units and locations where appropriate.

Effective Compliance MI presented to Executive committees by organisations should include:

- Regulatory risk assessment results and KRIs
- Results from compliance monitoring activity
- Updates on risk mitigation actions
- Updates of Compliance issues
- Policy breaches and notifiable events
- Treat Customer Fairly (TCF) metrics
- Incident reporting
- Product complaint trends
- Regulatory fines
- Consideration of new/revised regulatory requirements (horizon scanning)
- Compliance training actions.

Compliance MI should also be calibrated so that it is consistent with the risk appetite set by the board. This will ensure that the business reviews these metrics which best align to the risk appetite of the firm. Calibrating RAG triggers and including forward-looking metric will also be essential in ensuring senior management receive Compliance MI that is of maximum use to the business.

MI should be tailored to the size and operations of the business, with organisations having a global presence and wide service offerings generating a greater level of MI.

Typically, Compliance MI should be presented to executive level committees by the Head of Compliance (or equivalent member of the management team tasked with responsibility for regulatory compliance).

BOARD COMMITTEES

Submitting Compliance MI to the board, primarily via board sub-committees (Risk Committee, Audit Committee, or both), ensures key Compliance MI and regulatory compliance matters are escalated to board level attention.

In the majority of financial services organisations both the Board Risk Committee and the Board Audit Committee have a role in the oversight of Compliance matters. The FSA would expect to see some form of Compliance MI reporting into these committees.

Where Compliance MI is provided to both the Risk and Audit sub-committees, information tends to be split as follows:

- **Risk Committee: Regulatory risk MI**
- **Audit Committee: MI regarding the effectiveness of regulatory framework controls.**

Compliance MI presented to board sub-committees should be less detailed than that presented to executive level committees. However, its quality and quantity should be sufficient to enable senior management to understand how well the business is managing the regulatory risks to which it is exposed.

Typically, Compliance MI presented to these committees will be a summarised format of the information provided to executive level committees and should include:

- Material regulatory compliance matters
- Details of regulatory contact (including inspection, disciplinary matters and emerging development)
- Risk assessment results
- Compliance monitoring exceptions/any other monitoring of regulatory controls
- Updates on risk mitigation actions.

USE OF COMPLIANCE MI

An observable focus of FSA supervisory framework visits is not only on the quality of Compliance MI provided to senior management and the board, but also how that MI is used and challenged. Compliance MI therefore needs to be useable above all else.

If Compliance MI is neither challenged nor acted on by the business then it is debatable whether the Compliance environment is subjected to sufficient senior management scrutiny.

If firms are unable to demonstrate to the FSA examples of when Compliance MI presented has caused debate and challenge within executive level committees and the board, it is likely the FSA will view the MI as unfit for purpose or raise concerns over senior management’s oversight. Ensuring that MI is not only escalated but also actively debated is essential.

The frequency of board sub-committee meetings is also a key determinant in assessing how well Compliance MI is used by senior management. We would expect board sub-committees tasked with the oversight of regulatory compliance to meet at least four times per annum. This would be the minimum frequency required to demonstrate active and engaged senior management oversight of regulatory risks. The FSA’s opinion notwithstanding, we believe this minimum frequency of meetings to be good business practice as it allows for regular analysis and understanding of the firm’s risk profile.

KEY QUESTIONS TO CONSIDER

- Does your Compliance MI cover the range of regulatory risks to which the business is exposed and is it calibrated risk appetite?
- Does it provide to the senior management team a detailed understanding of whether the firm is compliant with the FSA’s rules?
- Given the FSA’s expectation that risk will be ‘owned’ by the board, are you confident that the level and detail of Compliance MI presented to the board is adequate to meet this expectation?
FOR THOSE FIRMS SUBJECT TO DUAL REGULATION BY [PRA] AND FCA, THEY WILL RECEIVE INDEPENDENT BUT COORDINATED SUPERVISION FROM FCA/PRA.

Clive Adamson, Director of Supervision, Conduct Business Unit, FSA, January 2012

INTERACTION WITH REGULATORS

Given the changes in the regulatory environment, supervisors are emphasising stress-testing of business plans, reviewing business models and scrutinising corporate governance and remuneration incentives. In this uncertain and shifting landscape, financial institutions need to develop closer relationships with supervisors and reach a shared understanding of what is required to meet these higher standards.
Regulators are unsurprisingly among the industry’s most important stakeholders, although the degree to which firms have in the past proactively fostered open and on-going communication with them has varied. Going forward, firms will need to ensure they have a defined protocol for managing their interaction with regulators, especially where oversight will be undertaken by both the PRA and the FCA. In general, the Compliance function should be the central hub via which all interaction with the regulator is channelled, ensuring that there is one contact with a full understanding of the regulator’s approach and of the standards to which the firm is held to account, and aware of all issues and communications between the various bodies.

Fostering this relationship, encompassing open dialogue and on-going communication, should help firms navigate the changing regulatory landscape and mitigate the potential for mis-interpretation of the regulatory rules and approach.

In analysing responsibilities for interacting with the regulator within the firms reviewed, we have sought to understand the impact of regulatory change on:

**Responsibility for interaction with the regulator**

**Responsibility for interaction with the regulator on prudential matters**

**Board and senior management oversight of interaction with the regulator.**

**RESPONSIBILITY FOR REGULATOR INTERACTION**

Maintaining open and constructive lines of communication with the regulator(s) is increasingly important. Firms that are best able to manage their relationship with regulatory stakeholders are likely to best adapt to changes in the regulatory structure.

Where a firm is dual regulated, we believe there should be one contact holding the relationship for both the PRA and FCA matters, as the two are often inter-linked. For example, any systemic failure with payment systems would affect prudential matters, and equally liquidity management and resolution recovery will have an impact on conduct. With the PRA and FCAs divergent objectives, it is key that one person acts in the firm’s interest to avoid the development of a chasm. We would expect this ultimate responsibility for liaising with the regulator to lie with the Head of Compliance, who has a full understanding of the organisation’s regulatory affairs.

Most important in designing a firm’s regulatory relationship structure is a clear understanding of roles and responsibilities. A key future aspect of interacting with the regulator(s) is the need to present a consistent message as to the firm’s regulatory risks and how these are being managed. This consistent message cannot be achieved if senior management is unclear who owns the relationship.

Currently ultimate responsibility for the relationship with the regulator is with one of the following:

- **Chief Risk Officer**
- **Board or Board Risk Committee**
- **Head / Regional Heads of Compliance.**

In the majority of cases in the financial services sector, the Compliance function presently owns the relationship and reports to the FSA on non-prudential matters. More often than not it is the Head of Compliance who interacts with the regulator, however some firms have a decentralised approach whereby the FSA maintains contact with individuals in each business area / function, meeting the Head of Compliance on a quarterly basis.

**KEY QUESTIONS TO CONSIDER**

- Are there clearly defined responsibilities for interaction with the regulator within your business?
- Is there a central point of contact who owns the relationship with your regulator supervisor? If not, how does the business ensure that consistent messages are being relayed to the regulator?
- How are you planning for regulatory interaction in the ‘twin peaks’ regulatory environment? Do you understand how this might work in practice, particularly in the event of dual regulation?

**RESPONSIBILITY FOR INTERACTION ON PRUDENTIAL MATTERS**

Our observations across retail banking and insurance show that it is common for Finance to have responsibility for prudential matters, due to the nature of the work. As such, conversations with the regulator are held directly with the Finance division, though it remains important that such conversations are shared with the Head of Compliance on a regular basis to facilitate awareness of all potential issues and coordination of consistent messages.

Firms should develop a more joined-up approach to interacting with the regulator(s), which involves a collaborative approach between Finance, Risk and Compliance.

**OVERSIGHT OF INTERACTION WITH THE REGULATOR**

We recommend that a committee, such as the Board Risk Committee, takes a role in the oversight and on-going monitoring of regulator interaction. The terms of reference of this committee should formally include the oversight of regulatory interaction and communication.

This requirement would provide a formal senior management forum which could assess on-going communication with the regulator(s) and also assess the cumulative impact of regulatory communication on the firm.

Currently, oversight is predominately achieved via the Board Audit or Risk Committee, which receive regular reports from Compliance with a summary of communications with the regulator. In some cases this varies by virtue of executive committee members conducting private meetings.

We recommend that regulatory interaction is reviewed and assessed at least monthly in order to provide to senior management a regular understanding of the messages communicated to the regulator(s) and all current open issues.

**KEY QUESTIONS TO CONSIDER**

- Does your board exercise oversight of the firm’s relationship with the regulator?
- If not, how does the business ensure the engagement of the board in communication with the regulator?
Please contact

Tim Howarth
Partner, Regulatory Risk Consulting
T: +44 (0) 20 7311 6640
E: tim.howarth@kpmg.co.uk

Iestyn Evans
Senior Manager, Regulatory Risk Consulting
T: +44 (0) 113 231 3173
E: iestyn.evans@kpmg.co.uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2012 KPMG LLP, a UK limited liability partnership, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved. Printed in the United Kingdom. The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.