

Compliance: A gap at the heart of risk management

Executive summary



PricewaterhouseCoopers Global Financial Services e-briefing programme

Welcome to the sixth in the series of our Financial Services e-briefing programme, entitled ***Compliance: A gap at the heart of risk management***. This e-briefing, written in association with the Economist Intelligence Unit, examines the wider issues and complexity of compliance in the financial services industry.

The research effort for this report comprised two key global initiatives:

- The Economist Intelligence Unit held over 20 one-on-one interviews with executives at international financial institutions, regulators and technology houses in the US, UK, Europe and Asia.
- The Economist Intelligence Unit and PricewaterhouseCoopers conducted a special online survey of senior executives in financial institutions on the subject of compliance. 160 executives from North America, Europe and Asia participated in the survey, which was conducted in June 2003.

The interview and survey findings were further supplemented by significant desk research.

I am confident that you will find this e-briefing thought-provoking and insightful. Soft copies of this report as well as the previous e-briefings on ***Wealth Management, Economic Capital, Risk Management, The Trust Challenge and IFRS*** are available, free of charge, from our web site www.pwc.com/financialservices

If you would like to have a more detailed discussion of the issues addressed within this e-briefing in relation to your firm please speak with your usual contact at PricewaterhouseCoopers. As ever, we would also appreciate your feedback on this e-briefing as this helps us to ensure that we are addressing the issues that you are most focused on.

Jeremy Scott
Chairman, Global Financial Services Leadership Team



From investment banks issuing misleading research to insurers misselling mortgages, a whole range of financial services organisations that don't lack for rules or compliance officers have fallen foul of the regulators and seen their franchises badly damaged. Something is clearly going wrong, but what?

- Behaviour that may be legally defensible can still damage the reputation of the business. A new global survey of 160 senior executives in the industry, undertaken especially for this briefing, reveals that compliance with government and exchange-mandated rules is seen as less important in avoiding reputational risk than internal codes of practice. Adhering to the law is necessary, but by no means sufficient, to protect against reputational risk. What's more, thanks to the importance and complexity of its products and services, the burden on financial services institutions to ensure that all reasonable steps are taken to protect consumer rights is much more onerous than in other industries.
- What is regarded as sharp practice by informed customers today often becomes the subject of regulation tomorrow – witness the proposals now before US legislators to oblige mutual-fund companies to publish clearer information about the costs they take out of people's savings. Following existing

rules is not enough; identifying and understanding the source and impact of potential regulations is just as critical.

- The compliance department alone cannot resolve the inherent conflict of interest between an organisation's desire for profits and its duty to wider stakeholders, including customers. Rules are meaningless if they go against the grain of the organisation as a whole – if, in other words, there is a culture of non-compliance.
- Compliance is often too reactive – the organisation changes only when rules do. Asked to identify the constituencies that drive the adoption and implementation of codes of best practice, for example, survey respondents put regulators well out in front. This kind of approach means compliance processes layer one upon the other, adding cost, increasing the likelihood of duplication and inconsistency, and reducing the overall agility of the business.

This briefing, written for PricewaterhouseCoopers by the Economist Intelligence Unit, argues that there is a gap between the processes that are designed to keep the organisation in line with its regulatory obligations and the policies that are needed to protect and burnish the franchise. 'A new vision of compliance is needed to bridge this gap,' says Juan Pujadas, leader of the global financial risk management practice at PricewaterhouseCoopers, 'one that puts the consumer first, that embraces internal guidelines as well as outside regulations,

that prevents damage to the franchise rather than just detecting it after the damage is done, and that embeds a culture of compliance into the marrow of financial institutions.'

A new definition of compliance risk

The risk of impairment to the organisation's business model, reputation and financial condition from failure to meet laws and regulations, internal standards and policies, and expectations of key stakeholders such as customers, employees and society as a whole.

This vision is slowly beginning to crystallise within the financial services industry and within the regulators, competition authorities and consumer groups that police it.

Regulators are moving towards real-time access to risk and compliance information and reporting and, in effect, towards looking over the shoulder of management as decisions are made. Their concept of compliance increasingly embraces internal management information and decision-making processes, from boardroom to front-desk.

Compliance: A gap at the heart of risk management

Executive summary *continued*



Things are also changing in the best-run financial services organisations. Rather than seeing compliance as a stand-alone, authorisation function, these institutions are now integrating compliance into their general risk management frameworks and making the management of regulatory risk a key part of effective overall compliance.

But too many institutions continue to fall short of first-class compliance, to judge by the results of the survey. Fewer than a fifth of surveyed organisations consider awareness of compliance-related risks to be high across all parts of the business. Fewer than a quarter are very confident that their organisation is in full compliance with regulatory requirements and internal codes and policies. That's deeply alarming – a string of high-profile examples in the financial services industry has underlined that a compliance failure in one part of the business can undermine the entire franchise.

The task of embedding compliance throughout financial institutions is undoubtedly a challenging one. 'The change necessary successfully to transform compliance requires a major cultural shift at all levels of an organisation, starting from the very top,' says Bob Moritz, leader of the US financial services practice at PricewaterhouseCoopers.

Three key principles stand out:

- 1** Board and senior managers must clearly articulate a vision of compliance that goes well beyond the compliance function itself and then drive the process of delivering on that vision. Clear and accessible policies and procedures must be deeply rooted in all business units and functions within financial institutions. Responsibility for compliance should be embedded throughout the enterprise from the most junior to the most senior person.
- 2** An infrastructure must be put in place to allow management to track current and emerging compliance issues and to communicate these to internal and external stakeholders. A comprehensive system of internal controls and audit must create an environment of continuous improvement in managing compliance risk. Part of the strategic process should be to review emerging trends in order to get 'ahead of the game' and anticipate new issues before they become embedded and difficult to address. Technology plays a critical role in this area, and the good news is that cost-effective solutions do exist.
- 3** Compliance must be used to drive value. Good compliance involves understanding and delivering on the expectations of customers and other stakeholders, thereby improving the quality of key relationships. Established and embedded compliance procedures makes new product and business

approval processes quicker, increasing strategic agility in a challenging marketplace. And more effective compliance strengthens the business model by lowering the risk premium and therefore the cost of capital.

Financial services organisations that fail to recognise and close the gap between the box-ticking approach to compliance and the totality of risks that they run are extremely vulnerable to reputational risk. 'Making compliance part of the enterprise-wide management framework – from strategy development through human resource management to all customer interactions – is critical to success,' concludes Phil Rivett, global leader of the banking and capital markets practice at PricewaterhouseCoopers.

Introduction



If there's one lesson that boards and senior managers should draw from the scandals that have rocked financial institutions over the past couple of years, it's this: the box-ticking approach no longer cuts it.

In the US, investment banks have long had internal guidelines that kept the research and investment banking sides of the business apart. Yet equity analysts recommended companies – many of them large clients of their investment-banking arms – that they considered to have major performance or management issues. The rules were in place, but they could not protect the franchise. The investment banks either ignored the rules or did not recognise the risks they were running by failing to address this conflict of interest.

Other examples abound. From the losses caused by rogue trading at a US subsidiary of Allied Irish Banks (AIB) to the fines imposed on a number of insurers for endowment mortgage misselling scandals in the UK, from the travails of securities houses in Japan to the inequitable allocation of stock offerings to preferred clients by investment banks during the market boom, a whole range of institutions that did not lack for rules or compliance officers have fallen foul of the regulators and seen their franchises badly damaged.

Compliance: A gap at the heart of risk management

You say Compliance, I say compliance



Something is clearly going wrong, but what? For a clue, listen to the thinking of a risk officer at one of the US banks to have been embroiled in the scandal over research recommendations. He describes compliance as a 'middle-office' function, providing an essential link between the salesmen of the front office and the technocrats of the back office. 'Compliance officers are the foot soldiers to the risk officers' generals,' he says. In other words, policymaking and risk identification are the work of risk departments and senior management, and compliance is simply there to tick things off against regulatory requirements.

That approach no longer holds. Increasingly, perceptive management teams in financial services firms are demanding that their compliance departments move from being just an authorisation function to adopting a more strategic outlook, broadening its remit to cover internal codes of conduct, regulatory risk management and areas beyond just financial regulation.

But there's a more fundamental problem. The compliance department alone cannot resolve the inherent conflict of interest between an organisation's desire for profits and its duty to wider stakeholders, especially customers. Would Nick Leeson have brought Barings to its knees if he hadn't been regarded as a star trader? At the US investment banks, would analysts have issued the recommendations they did if they had not been encouraged to do so by aggressive pay packages that rewarded short-term performance? Would the UK pensions misselling scandal have happened if salesmen had not reaped substantial upfront commissions for pushing particular policies? Rules are meaningless if they go against the grain of the organisation as a whole – in other words, if there is a culture of non-compliance.

There is a gap between the processes that are designed to keep the organisation in line with its regulatory obligations and the policies that are needed to protect and burnish the franchise as a whole. 'A new vision of compliance is needed to bridge this gap,' says Juan Pujadas, a partner at PricewaterhouseCoopers, 'one that puts the consumer first, that embraces internal guidelines as well as outside regulations, that prevents damage to the franchise rather than just detecting it after the damage is done, and that embeds a culture of compliance into the marrow of financial institutions.'

Image rights



This vision is slowly beginning to crystallise within the financial services industry and the regulators who police it.

According to a global survey of 160 senior financial services executives undertaken especially for this report, reputational risk is now the single biggest risk financial institutions face. Even if reputational risk can be seen as a secondary risk arising from other types of risk, such as operational risk or regulatory risk, arguments over taxonomy should not obscure the fact that this is the industry's greatest source of worry.

How important are the following risks to your institution's financial services business? (% of respondents rating each risk as the biggest risk their organisation faces)

Reputational risk	53%
Credit risk	34%
Regulatory risk	28%
Operational risk	24%
Market risk	23%
Political/external risk	11%

Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June 2003

In part, that reflects the growing assertiveness and increased willingness of regulators and others to rap institutions very publicly over the knuckles for management failures – witness the high-profile pursuit of wayward US investment banks by the New York state attorney. In part, it reflects more intrusive scrutiny from consumer groups, customers, shareholders and media into issues of governance and risk management, and their growing capacity to influence the regulatory debate and management decisions.

Addressing these challenges requires more of financial institutions than sticking to the letter of the law.

Asked to identify the policies that do most to mitigate reputational risk at financial institutions, the survey group picked clear and accessible codes of governance and risk management practices and effective internal controls. Explicit shared responsibility among staff for adherence to codes of conduct, regulations and best practices came next. Revealingly, having a properly resourced compliance function came only fourth in the pecking-order.

Which of the following does most, in your view, to mitigate reputational risk at financial institutions? (% of respondents)

Clear and accessible codes of governance and risk management practices	64%
Effective internal controls	60%
Explicit shared responsibility among staff for adherence to codes of conduct, regulations and best practices	48%
A properly resourced compliance function	36%
Clear complaint and redress procedures	23%
Good performance	23%
Clear statements of risk appetite	21%
Respected partners	16%
Clear and transparent compensation schemes	12%
Fair treatment of whistleblowers	11%
Other (please specify)	3%

Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June 2003

Respondents also agreed that compliance with internal risk control policies is more important than compliance with government – or exchange-mandated regulations in mitigating reputational risk. They're right.

Compliance: A gap at the heart of risk management

Image rights *continued*



For one thing, the rules don't always go far enough. Behaviour that is acceptable in the eyes of the law can still be illegitimate in the eyes of customers and other stakeholders. 'The secret is to put yourself in the shoes of the average consumer and see if you still pass the smell test,' says Phil Rivett, a partner at PricewaterhouseCoopers. The word 'average' is important in this respect – selling to sophisticated institutional investors within the industry is one thing, but explaining the ups and downs of complex financial products to the man in the street quite another. More than 12m people in the UK currently invest directly in stocks and shares, for instance, but according to Department of Education statistics, as many as 29% of adults, or 11m people, in the UK cannot calculate the area of a floor. 'Meeting the legal requirements of disclosure is not enough to explain the risks of investment to consumers who lack basic numeracy skills,' says Tony Evangelista, head of the US investment management regulatory compliance group at PricewaterhouseCoopers.

Of course, the principle of 'buyer beware' is not dead yet (as the recent dismissal of a class action lawsuit against Wall Street banks by disappointed investors demonstrated). But what is regarded as sharp practice by informed customers today often becomes the subject of consumer pressure and then regulation tomorrow.

Financial institutions that aim to do the right thing by their customers have a better profile and are likelier to be in pre-emptive compliance with regulators than those that do the minimum required by law. Take the proposals now before US legislators to inject greater transparency into the fund-management industry by obliging mutual-fund companies to publish clearer information about the costs they take out of people's savings. A fund that already makes its costs transparent would have no need to alter its behaviour and will almost certainly have happier customers – Legal & General, a UK insurer, has recently increased its levels of client satisfaction significantly by applying 'plain English' guidelines to the statements sent to customers explaining how with-profits bonds work and how the underlying assets were performing.

Empowering everyone



Running through the survey respondents' answers is an awareness that the responsibility for sound business management rests not just with those in the compliance department or even the traditional risk disciplines, but with everyone in the organisation. Internal controls embed compliance in people's roles and responsibility more effectively than external regulations. Although the personal liability of senior managers for regulatory non-compliance has risen exponentially in the last two years, the mindset of employees lower down the management chain is different – thinking about regulations is not their concern, but the job of the compliance department.

Internal codes of business practice are intuitively different – they manifestly apply to everyone in the institution. Only through internal controls can a culture of compliance become embedded throughout the organisation (a theme discussed in a previous e-briefing, *Taming uncertainty: Risk management for the entire enterprise*). According to Rick Heathcote, a partner in the compliance risk management practice in

Hong Kong for PricewaterhouseCoopers, 'An overly rigid separation between the responsibilities of the compliance department and the activities of the risk management team leaves institutions vulnerable to the very compliance failures they are designed to prevent.'

Regulators themselves acknowledge that institutions have a greater awareness of the risks that they run and the safeguards they need to put in place than anyone else. There is a clear trend towards continuous and risk-focused supervision in financial services regulation. Regulators are moving increasingly towards real-time access to risk information and reporting at the firm level – in effect, they want to look over the shoulder of management as decisions are made, exposing internal information and decision-making processes to deeper scrutiny than ever before.

The requirements of the Sarbanes-Oxley Act in the US, for example, include the obligation to set up and maintain adequate financial reporting controls and procedures. The thrust of Section 404 of Sarbanes-Oxley, towards developing an internal governance structure that enables risks to be properly monitored and reported, runs largely parallel to Basel II compliance risk reporting requirements. Similar requirements already exist in many countries in relation to the controls and procedures in financial service organisations. The focus provided by Sarbanes-Oxley will

help ensure that these are in practice operating to the level intended by the regulators. So too will the expanding requirements of anti-money laundering and know your customer regimes around the world.

In another clear move toward industry self-regulation, a US Securities and Exchange Commission (SEC) proposal from February 2003 would require each investment company and investment adviser registered with the Commission to adopt and implement policies and procedures reasonably designed to prevent violation of the federal securities laws, to review those policies and procedures annually for their adequacy and the effectiveness of their implementation, and to appoint a chief compliance officer to be responsible for administering the policies and procedures.



Regulatory risk – a new risk management discipline?

Compliance with regulatory requirements is the first step in effective overall compliance. But it's easier said than done. The sheer complexity of the regulatory environment is seen by survey respondents as the biggest single barrier to achieving first-class overall compliance and the burden is worsening – half the respondents think that regulatory pressures will increase substantially over the next three years.

Globalisation of markets means that one financial institution can be interacting with and subject to the rules of literally hundreds of financial services and other regulators. Speed of business transformation means that rules are being changed more frequently. An increased focus on risk and governance issues throughout the global economy is driving a host of new transnational regulatory initiatives.

'As a result, the effective identification and management of regulatory risk as a key component of effective overall compliance is now taking shape as a risk discipline in its own right' says Andy Turner, a partner in the financial services regulatory practice in the UK for PricewaterhouseCoopers. Mr Turner defines regulatory risk as 'the risk of material loss, reputational damage or liability arising from failure to

comply with the requirements of the regulators or related codes of best practice that oversee regulated business in whatever areas the organisation operates'.

Regulatory risk impacts on regulated businesses in any industry and can be broken down into:

- **Upstream risks** – risks that exist before rules are made. These include the risks that the organisation is unaware of potential regulatory developments, that it fails to assess the commercial and regulatory impact of new legislation, that it fails to lobby legislators and regulators effectively and that it fails to plan and implement new rules effectively.
- **Downstream risks** – risks that exist after rules are made. These include the risks that existing rules are not being complied with in the organisation, that changes in the organisation's business scope are affected by existing or new types of rules or regulators and that breaches identified in the organisation are not rectified promptly.
- **Regulator risk** – the risks of not developing and managing effective relationships with regulators. These include weakened lobbying impact, an overly intrusive supervision process and avoidable enforcement action.

The traditional compliance or risk management functions may well be the natural functions to take primary responsibility for the management of those key regulatory risks. But critically, these are not technical issues to be delegated and then forgotten about.

Senior management and the relevant board committees must remain closely involved, not just because the costs of ineffective management of downstream risks can be so high but also because the effective management of upstream risks and regulatory relationships at very senior levels will enable the organisation to assess and influence most effectively the changing regulatory landscape.

The compliance gap



So executives and regulators agree that good compliance involves more than ticking the boxes on a regulatory handbook. But the survey offers little comfort that this realisation is being translated into effective action throughout institutions.

Respondents doubted the effectiveness of their own compliance procedures. Just 28% thought their procedures were extremely effective at ensuring the firm was in compliance with regulations or with internal policies and procedures, a damningly small proportion. Significant minorities rated their compliance procedures as ineffective or extremely ineffective at influencing the regulatory process and building greater confidence in the organisation on the part of clients. And few executives thought that compliance procedures were helping to unlock strategic business value.

Within your own organisation, how effective are your compliance procedures in meeting the following goals? (% of respondents rating procedures as ineffective or extremely ineffective)

Influencing the regulatory process in the interests of the firm	25%
Acting as the champion of the customer within the firm	22%
Building greater confidence in the organisation on the part of clients	21%
Acting as a central repository for all information on rules, codes of conduct and business practices, and ensuring dissemination to all appropriate people in the organisation	13%
Training and educating staff in regulatory requirements and requirements of internal policies and procedures	12%
Ensuring that the firm abides by its own policies and procedures	8%
Ensuring that reputational risk is being managed effectively	7%
Ensuring that regulatory risk in the institution is being managed effectively	7%
Ensuring that the firm is in compliance with regulations	5%

Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June 2003

Far from embedding a culture of compliance throughout the organisation, fewer than a fifth of respondents say that awareness of compliance-related risks is high in all parts of the business. Only 60% believe that all or most parts of the business are well-informed. In other words, 40% of the institutions surveyed acknowledge that significant areas of their business operate without clear knowledge of the compliance-related risks they run. Fewer than a quarter of respondents are very confident that their organisation is in full compliance with regulatory requirements and internal codes and policies.

How do you rate your institution's level of knowledge about the compliance-related risks you face? (% of respondents)

Most parts of the business are well-informed about the compliance-related risks we face	45%
Some parts of the business are well-informed about the compliance-related risks we face	28%
All parts of the business are well-informed about the compliance-related risks we face	15%
Only the risk/compliance department is well-informed about the compliance-related risks we face	10%
No parts of the business are well-informed about the compliance-related risks we face	1%
Don't know	1%

Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June 2003

Compliance: A gap at the heart of risk management

The compliance gap *continued*



This is deeply concerning, and not just for the institutions that run the risk of seeing their franchise disappear. It's also a cause of concern for the wider economy. As we argued in a previous e-briefing, *The trust challenge: How the management of financial institutions can lead the rebuilding of public confidence*, the financial services industry has a leadership role to play in restoring the public's belief in the integrity of companies and financial markets. It cannot take up that role unless its own risk management and governance procedures are up to scratch. Yet many institutions are still failing to adopt a pro-active approach to the challenge – asked to identify the constituencies that drive the adoption and implementation of codes of best practice, respondents put firms themselves a lowly fifth, behind regulators, customers, governments and shareholders.

Which constituencies are the key drivers of initiatives to adopt and implement codes of best practice within financial services institutions, in your view? (% of respondents)

Regulators	76%
Customers	48%
Governments	45%
Shareholders	30%
Firms	28%
Trade and lobbying associations	20%
Media	14%

Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June 2003

The way ahead



Not all institutions are so passive, however, and three key attributes mark out institutions that are in the vanguard on compliance risk management:

- 1 Compliance is broadly defined and responsibility for compliance is widely shared.
- 2 Technology is a key enabler of compliance risk management.
- 3 Compliance is used to drive value.

Compliance is broadly defined and responsibility for compliance is widely shared.

'Compliance' continues to mean different things to different people. The executives we surveyed for this report exemplify the confusion: asked to identify the goals of compliance, no clear view emerged. The top answer – to ensure that the firm is in compliance with regulations – was still picked by fewer than half of the survey group.

The lack of consensus reflects the fact that compliance ought to embrace an array of goals, not just one. Juan Pujadas of PricewaterhouseCoopers offers this working definition of compliance risk: 'The risk of impairment to the organisation's business model, reputation and financial condition from failure to meet laws and regulations, internal standards and policies, and expectations of key stakeholders such as customers, employees and society as a whole'. Defined thus, compliance risk management is increasingly aligned with operational risk – indeed, Mr Pujadas describes compliance as 'operational risk come alive'. This alignment underscores the need for compliance risk management to reach throughout the business.

What, in your view, should the primary goals of compliance within a financial institution be? (% of respondents)

To ensure that the firm is in compliance with regulations	46%
To ensure that regulatory risk in the institution is being managed effectively	33%
To train and educate staff in regulatory requirements and the requirements of internal policies and procedures	30%
To ensure that the firm is abiding by its own policies and procedures	27%
To ensure that reputational risk is being managed effectively	26%
To help the firm anticipate and plan for changes in regulations	20%
To act as a central repository for all information on rules, codes and business practices and ensure dissemination to all appropriate people in the organisation	16%
To build greater confidence in the organisation on the part of clients	13%
To act as the champion of the customer within the firm	5%
To influence the regulatory process in the interests of the firm	5%

Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June 2003

Compliance: A gap at the heart of risk management

The way ahead *continued*



At Goldman Sachs – where operational risk is defined as ‘the risk of reputational damage, regulatory intervention or financial loss resulting from inadequate or failed internal processes or systems’ – the Global Compliance and Control Committee, whose members include senior members of the firm’s business units, helps in the identification and review of certain ‘compliance, reputational and other operational risks’ and in the development of policies and communication and training programmes designed to mitigate these risks. At Citigroup, each major business line must have specific policies and procedures for ensuring compliance with corporate policies and relevant laws and regulations. At UBS, Barclays, LloydsTSB, the Royal Bank of Scotland and others, the compliance department has changed from being a stand-alone division to being tightly integrated into the general risk management structure (see box overleaf).

Not everyone likes the idea of a cosier relationship between the compliance department and the general risk management team. ‘Risk management is a part of general management, and the compliance department must be an independent cop charged with monitoring management behaviour and policies,’ says Professor David Llewellyn of Loughborough University in the UK.

That’s arguable. Internal audit could play the same role, after all. Cultural norms, such as an environment that rewarded

whistleblowing, are more likely to prevent or spot governance failures. And when two of the key barriers to achieving first-rate compliance identified in the survey are poor integration between the compliance function and other functions, and the perception that compliance is not a universal responsibility, ring-fencing compliance carries more dangers than integrating it.

Others worry that the principles of risk management, which involve gauging risk appetite and imply a willingness to accept that some things will go wrong, may erode a culture of zero tolerance for compliance failures. Some leading financial institutions are already calculating an economic capital charge for operational risk, enabling companies, and their stakeholders, to gain a better understanding of their appetite for risk and where they are prepared to accept volatility or uncertainty in exchange for high returns. In emerging markets in particular – where, as Antony Eldridge, a partner in the financial services practice in Japan for PricewaterhouseCoopers, points out, regulations are often unclear and there is ample wiggle-room for interpretation – institutions may choose not to mitigate every compliance risk fully in order to maintain an adequate level of profits.

When the consequences of a compliance failure can be so dramatic, might the risk management approach offer false comfort?

Responsibility for addressing this problem rests firmly with senior management. ‘If senior managers set crystal-clear parameters about acceptable and unacceptable behaviour throughout the enterprise, the risk control framework will not be undermined’, says John Scheid, leader of the global insurance, assurance and advisory practice at PricewaterhouseCoopers. In addition, senior managers will do a better job of defining the organisation’s risk appetite and culture if they have the fullest possible information on the nature, probability and likely impact of the risks they face. Keeping compliance in a narrow functional box is not the way to improve these flows of information.



UBiquitous

Switzerland's UBS is one organisation to have enmeshed its compliance function into its risk management framework. A couple of years ago, UBS rejigged things so that its group compliance officer, Neil Stocks, reported directly to Walter Stürzinger, the group's chief risk officer, and through him to the president of the executive board.

Previously, there had been a combined legal and compliance department, and the integration of the compliance department was part of UBS's general attempts to improve risk management, particularly in areas where there were perceived to have been weaknesses in the past. Core to its thinking was that it had to take all types of risk into account, and in particular intangible risks to reputation and the like. It has done so by involving all departments, even public relations, in risk and new project assessment.

'Whilst the advisory role of compliance was clearly of importance,' says Mr Stürzinger, 'we decided that the function should also play a more pro-active role in risk control.' Compliance has therefore been folded into this broad approach to risk management. At group level, Mr Stocks is therefore involved in the vetting of proposed transactions, taking into account internal guidelines as well

as outside regulatory requirements when deciding whether to give a project the go-ahead.

Mr Stocks can advise against a deal, but the right of veto generally rests with Mr Stürzinger. There have been examples of deals which have been rejected on Mr Stocks' advice, where, for example, a due diligence process has revealed potential ethical or reputational problems.

Mr Stocks identifies three core elements to his job:

- 1 Keeping an eye on regulatory relationships, although adherence to national regulations is the direct responsibility of the relevant local office.
- 2 Maintaining an overview of compliance requirements and resources and making sure that individual business groups have the necessary support.
- 3 Making sure that the group gets to know of problems and regulatory requirements in good time 'and hopefully before an incident hits the press'.

There is little radically new in this list, but it does imply that the scope of compliance at UBS has widened well beyond a purely box-ticking approach, which only considers whether the bank is breaking the letter of the law or regulation.

The particular challenge, says Mr Stocks, is effectively to anticipate regulatory problems before they become an issue. You must keep in very close touch with regulators and other market players, he says, 'and try to work out where they want you to be'.

No easy task, but UBS claims that such thinking helped it avoid some of the regulatory problems that have beset the US investment banking world. UBS has also recognised that compliance should include staff with varied backgrounds, as well as lawyers and accountants. 'You need generalists who can take the broad view', says Mr Stürzinger, and Mr Stocks makes his point for him: before taking his present job, he headed up the UBS Private Bank in London.

Compliance: A gap at the heart of risk management

Technology is a key enabler of compliance risk management



As in other areas of risk management, technology is critical to effective compliance. First, communications technologies play a vital role in disseminating internal codes of practice and other compliance-related information and in reinforcing a culture of compliance within the organisation. From placing best practice documents on the corporate intranet to using pop-up messages to query transactions or wording that sit outside defined parameters, technology can push the compliance burden out to all parts of the business (see box overleaf).

Second, technology is key, particularly in large, complex organisations, to collecting, measuring and monitoring the data upon which risk management processes are built. This data is used to detect breaches of regulations and to identify areas that may point to future sources of regulatory risk, such as a particular concentration of customer complaints.

Third, technology can deliver management information to internal decision-makers and to external stakeholders in cost-effective formats that enable instant analysis of compliance risk. 'Recent corporate information failures and accounting

irregularities mean that the legislative and regulatory noose is tightening for all the directors of public corporations,' says Robert Bittlestone, managing director of Metapraxis, a consultancy and software group.

Metapraxis has launched a new monthly professional service called the Directors' Early Warning Service, aimed at helping both executive and non-executive directors to detect current and potential performance problems or financial irregularities. The service provides an automated monthly scan across the internal results and forecasts of each subsidiary of a major corporation. This is coupled with econometric and statistical analyses to highlight issues such as suspicious or unusual data, dangerous trends and high-risk forecasts. 'Organisations can now see the big picture without having to wade through mountains of numeric paper reports,' says Mr Bittlestone. 'You can find out in four weeks what it would normally take you a year to discover, by which time it's too late.'

The emergence of Extensible Business Reporting Language (XBRL), a new programming language that uses standard data tags to identify different pieces of information within a firm's financial data set, is another very significant development. Financial managers know they must develop, distribute and analyse financial and business reports quickly – timely information can be the difference between success and failure.

The introduction of XBRL will improve the management and distribution of needed data to the whole value chain of financial institutions.

For firms that labour under a variety of regulatory reporting regimes, XBRL holds out the promise of being able to submit financial data to a number of regulators in a single format. The application of XBRL has been pioneered for regulatory reporting purposes by the Australian Prudential Regulatory Authority (APRA). Regulated entities have to report financial and statistical data to a number of regulatory bodies, all of which require the data to be sent in a different format. APRA acts as a 'pass-through' agency and sends the data to these other regulatory bodies on behalf of the firms it regulates. APRA now collects data in XBRL from many of its regulated firms, reducing the costs of gathering and analysing the data for itself and passing these cost benefits back to its regulated entities.

In the US, the Federal Deposit Insurance Corporation (FDIC) has already reached agreement to build a new Internet-based central data repository for call reporting and other regulatory reports using the XBRL data standard. And with the advent of Sarbanes-Oxley, the SEC may well adopt the standard in the future.

Compliance: A gap at the heart of risk management

Technology is a key enabler of compliance risk management *continued*



Gatekeepers

In June of this year, Autonomy, a California-based software house, launched a new division. Called Aungate, the Cambridge, UK division produces software aimed specifically at compliance departments, and a number of big financial institutions have already snapped up its products.

The technology can be used to monitor everything from telephone conversations to e-mails for potential regulatory and legal violations. What's more, it can do so in real time. Set it up to monitor mentions of a particularly sensitive client, for example, and it flashes up a warning message before the e-mail is sent, alerting the writer to potential dangers.

Investment banks can check whether companies recommended by their research departments are doing a suspiciously high number of transactions with the bank, for example, or know instantly if unusually high commissions are being charged for some business.

Equally, all calls and e-mails can be monitored instantly, and unusual patterns spotted, whereas old-fashioned manual checking could cover only a tiny proportion of such calls. As a result, the system helps prevent future problems, whereas manual systems were largely used to investigate past events.

Interestingly, there's actually little new about Aungate's product. What is new is that it is being sold to compliance departments, as regulators start to insist that firms in general, and banks in particular, document the effectiveness of internal controls, and supply detailed risk assessment data. Most simply can't do so at the moment. According to Aungate's communications director, Ian Black, 80% of financial institutions do not yet meet SEC compliance regulations, for example.

Compliance: A gap at the heart of risk management

Compliance is used to drive value



A culture of compliance does more than mitigate risk. It also realises value. Being able to demonstrate that they comply with regulations and internal codes of conduct helps institutions to enhance their reputation as practitioners of good business among customers and employees – witness the value of SAS70 and FRAG21 reports on internal control environments to investment management firms and custodians. It can also enable organisations to manage relationships with key stakeholders more effectively – compliance with know your customer rules for anti-money laundering purposes, for example, can substantially improve the quality of customer relationship management.

Compliance risk management can also enable greater agility. Take the new product and new business approval processes. Instituting a risk charter with which each new product and business must comply imposes discipline on the process but

also enables fast-track approval for projects that meet the appropriate criteria.

And it can also reduce losses, in effect freeing up capital. Citigroup said in December 2002 that it would set aside \$1.3bn for regulatory settlements and private litigation: its share of the industry's settlement with the regulators over misleading investment bank research accounted for only \$400m of this. Chubb put \$100m into its reserves for D&O-related losses in the fourth quarter of last year. Credit Suisse First Boston said in January that it put \$450m into reserve for private litigation alone. Those provisions could be reduced if organisations had more confidence in their standards of compliance.

Compliance: A gap at the heart of risk management

Conclusion



Financial services institutions that fail to meet the expectations of their regulators, stakeholders and customers will almost certainly create strategic and tactical impediments for themselves – indeed they can risk losing their franchise. To avoid such setbacks, institutions must identify and aggressively manage all areas of operating risk.

Increasingly, that means taking a new approach to compliance, one that elevates it beyond a specific function and enmeshes it deep within an institution's risk management DNA. In a regulatory environment where compliance is increasingly synonymous with the quality of operational risk management and in a marketplace where damage to the reputation of an institution is quickly inflicted and slowly healed, all parts of the business must be aware of and take responsibility for compliance-related risks.

Our survey results suggest that too many institutions continue to lag far behind this ideal. The losses that they risk running as a result are potentially heart-stopping. The value they lose in terms of their reputation with customers and other stakeholders will lead, perhaps more gradually, to the same end. According to Phil Rivett of PricewaterhouseCoopers, 'Making compliance part of the enterprise-wide management framework – from strategy development through human resource management to all customer interactions – is critical to success and the elimination of reputational risk.' Put like that, compliance is just too important to get wrong.

Appendix: Survey results



The Economist Intelligence Unit and PricewaterhouseCoopers conducted a special online survey of senior executives in financial institutions on the subject of compliance. Executives from 160 financial institutions in North America, Europe and Asia participated in the survey, which was conducted in June 2003. Our thanks are due to all those who responded, for sharing their insight with us.

Please note that totals do not always add up to 100 because of rounding, or because respondents could choose more than one answer.

About you

1. Where are you located?

Western Europe	29%
North America	20%
Asia-Pacific	33%
Middle East/North Africa	5%
Eastern Europe	7%
Latin America	6%
Sub-Saharan Africa	1%

2. What is your area of responsibility?

Senior management	23%
Finance	14%
Risk management	9%
Strategy/planning	11%
Compliance	23%
Marketing and communications	6%
Operations	3%
Legal	1%
Internal audit	3%
Other (please specify)	9%

3. What area of financial services do you personally work in? Please check as many areas as apply

Retail banking	23%
Investment banking	25%
Insurance	30%
Investment management	33%
Capital markets	18%
Private equity	15%
Corporate banking	28%
Private banking	16%
Other (please specify)	14%

4. What were your organisation's revenues, in US dollars, in 2002?

Less than \$500m	42%
\$500m-\$1bn	10%
\$1bn-\$3bn	14%
\$3bn-\$8bn	8%
Over \$8bn	21%
Not applicable	6%

5. How many different financial services regulators is your organisation subject to around the world?

Under 10	57%
10-25	11%
25-50	10%
50-75	6%
75-100	4%
Over 100	11%

Appendix: Survey results *continued*



The risk environment

6. How important are the following risks to your institution's financial services business? Please rate each risk between 1 and 5, 1 being the biggest risk your organisation faces and 5 being an insignificant risk.

	1	2	3	4	5
Reputational risk	53%	30%	12%	3%	2%
Credit risk	34%	23%	19%	16%	7%
Regulatory risk	28%	35%	26%	8%	3%
Operational risk	24%	35%	30%	8%	3%
Market risk	23%	45%	22%	9%	2%
Political/external risk	11%	33%	35%	16%	5%

7. How effective is compliance as a risk management tool in tackling each of the following risks? Please rate the effectiveness of compliance between 1 and 5, 1 being extremely effective and 5 being ineffective.

	1	2	3	4	5
Regulatory risk	40%	36%	18%	4%	1%
Reputational risk	26%	41%	24%	8%	1%
Credit risk	19%	38%	26%	11%	6%
Operational risk	14%	46%	31%	6%	3%
Market risk	13%	36%	27%	18%	6%
Political/external risk	5%	25%	38%	22%	10%

8. In your view, is the regulatory pressure on financial institutions likely to increase or decrease over the next three years?

Increase substantially	50%
Increase slightly	39%
Stay the same	8%
Decrease slightly	2%
Decrease substantially	1%

9. Which constituencies are the key drivers of initiatives to adopt and implement codes of best practice within financial services institutions, in your view?

Regulators	76%
Customers	48%
Governments	45%
Shareholders	30%
Firms	28%
Trade and lobbying associations	20%
Media	14%

10. How do you rate your institution's level of knowledge about the compliance-related risks you face? Please choose one answer.

Most parts of the business are well-informed about the compliance-related risks we face	45%
Some parts of the business are well-informed about the compliance-related risks we face	28%
All parts of the business are well-informed about the compliance-related risks we face	15%
Only the risk/compliance department is well-informed about the compliance-related risks we face	10%
No parts of the business are well-informed about the compliance-related risks we face	1%
Don't know	1%

Appendix: Survey results *continued*



11. Which of the following does most, in your view, to mitigate reputational risk at financial institutions? Choose the top three answers.

Clear and accessible codes of governance and risk management practices	64%
Effective internal controls	60%
Explicit shared responsibility among staff for adherence to codes of conduct, regulations and best practices	48%
A properly resourced compliance function	36%
Clear complaint and redress procedures	23%
Good performance	23%
Clear statements of risk appetite	21%
Respected partners	16%
Clear and transparent compensation schemes	12%
Fair treatment of whistleblowers	11%
Other (please specify)	3%

12. Which is more important, in your view, in ensuring that a financial institution avoids reputational risk?

Compliance with internal risk control policies	62%
Compliance with government and/or exchange-mandated rules	38%

The role of compliance

13. What, in your view, should the primary goals of compliance within a financial institution be? Please choose the top two goals.

To ensure that the firm is in compliance with regulations	46%
To ensure that regulatory risk in the institution is being managed effectively	33%
To train and educate staff in regulatory requirements and the requirements of internal policies and procedures	30%
To ensure that the firm is abiding by its own policies and procedures	27%
To ensure that reputational risk is being managed effectively	26%
To help the firm anticipate and plan for changes in regulations	20%
To act as a central repository for all information on rules, codes and business practices and ensure dissemination to all appropriate people in the organisation	16%
To build greater confidence in the organisation on the part of clients	13%
To act as the champion of the customer within the firm	5%
To influence the regulatory process in the interests of the firm	5%
Other (please specify)	1%

14. How important is compliance within the culture of your organisation?

Very important	46%
Essential	33%
Important	19%
Not important	2%

15. How confident are you that your organisation is in full compliance with its regulatory requirements and with its own codes, practices and policies?

Confident	66%
Very confident	21%
Not confident	13%
Don't know	1%

Compliance: A gap at the heart of risk management

Appendix: Survey results *continued*



16. In your view, what are the secrets of good compliance within a financial services organisation? Please choose as many answers as apply.

Clear internal codes of conduct and business practice	86%
Emphasis on compliance from senior managers	74%
Responsibility for compliance is widely shared	62%
Availability of proper management data and information	55%
Use of technology to monitor and identify compliance issues	50%
Compliance function is properly staffed and funded	48%
Good relationships with regulators	31%
Other (please specify)	4%

17. Within your own organisation, please rate the effectiveness of your compliance procedures in meeting the following goals. For each goal, please rate between 1 and 5, 1 being extremely effective and 5 being extremely ineffective.

	1	2	3	4	5
Ensuring that the firm is in compliance with regulations	28%	49%	19%	2%	3%
Ensuring that the firm abides by its own policies and procedures	28%	41%	24%	7%	1%
Training and educating staff in regulatory requirements and requirements of internal policies and procedures	18%	31%	39%	10%	2%
Ensuring that reputational risk is being managed effectively	16%	47%	30%	6%	1%
Acting as a central repository for all information on rules, codes of conduct and business practices, and ensuring dissemination to all appropriate people in the organisation	16%	40%	32%	10%	3%
Ensuring that regulatory risk in the institution is being managed effectively	15%	50%	28%	6%	1%
Acting as the champion of the customer within the firm	12%	28%	38%	18%	4%
Helping the firm anticipate and plan for changes in regulations	11%	45%	31%	11%	1%
Building greater confidence in the organisation on the part of clients	8%	34%	38%	18%	3%
Influencing the regulatory process in the interests of the firm	5%	32%	38%	14%	11%

Appendix: Survey results *continued*



18. In your view, is compliance handled in a cost-effective manner in your organisation?

Yes	71%
No	29%

19. What are the key benefits of first-rate compliance, in your view? Please check the top two benefits.

The firm avoids damage to its reputation stemming from non-compliance	82%
The firm avoids financial and other penalties stemming from non-compliance	53%
The firm's overall strategy is less susceptible to operational risk	39%
The firm is likelier to be responding to the wishes and needs of the customer	23%
The firm has access to better management information	7%

20. What are the key barriers to achieving first-rate compliance, in your view? Please check the top two barriers.

Sheer complexity of regulatory environment	47%
Poor integration with other functions, including risk management, sales and customer service	36%
Perception that compliance is not a responsibility of every member of staff	31%
Perception that compliance is not a strategic function	26%
Focus on cost-cutting in the current environment	23%
Inadequate technological infrastructure for monitoring compliance	16%
Lack of direct communication between compliance and senior management	15%
Insufficient pool of talent in this area of the business	10%
Other (please specify)	3%

The compliance function

21. Which department in your organisation has primary responsibility for compliance? Please check all that apply.

Specific compliance department	42%
Legal	38%
Internal audit	33%
Risk	29%
Finance	23%
We outsource regulatory compliance	3%
Other (please specify)	8%

22. To what extent is compliance in your organisation centralised? Choose as many answers as apply.

Largely centralised on a global level	29%
Largely centralised at a regional level	25%
Largely decentralised to local territories	14%
Largely centralised at a group level	19%
Largely centralised at the level of the business	16%
Largely decentralised to individual divisions	14%

Compliance: A gap at the heart of risk management

Appendix: Survey results *continued*



23. How do you evaluate the current status of the compliance function within your organisation?

	Low	Average	High
Stature of department	13%	68%	20%
Quality of compliance staff	11%	52%	37%
Numbers of compliance staff	35%	54%	11%
Size of budget	34%	59%	7%

24. To whom does your chief compliance officer report?

Chief executive officer	35%
Head of legal	18%
We don't have a chief compliance officer	16%
Chief risk officer	9%
Chief finance officer	9%
Head of internal audit	4%
Other (please specify)	8%

25. Is the compliance function in your organisation involved in the new product approval process?

Yes	62%
No	38%

26. Does your organisation have metrics to gauge the return on its investment in compliance?

Yes	22%
No	78%

Compliance: A gap at the heart of risk management

Contacts



If you would like to discuss any of the issues raised in this survey in more detail please speak with your usual contact at PricewaterhouseCoopers or call one of the following:

Compliance: A gap at the heart of risk management e-briefing editorial board

Etienne Boris*

33 1 56 57 1029

etienne.boris@fr.pwc.com

Andrew P. Clark

44 20 7804 5761

andrew.p.clark@uk.pwc.com

Antony M. Eldridge

81 3 5532 2519

antony.m.eldridge@jp.pwc.com

Tony Evangelista

1 646 471 7380

tony.evangelista@us.pwc.com

Andrew R. Gordon

44 20 7804 4187

andrew.gordon@uk.pwc.com

Rick Heathcote

852 2289 1155

rick.heathcote@hk.pwc.com

Michael Knoll

41 1 630 15 36

michael.knoll@ch.pwc.com

Bob Moritz*

1 646 471 8486

robert.moritz@us.pwc.com

Edward J. Muhl

1 202 414 1490

edward.j.muhl@us.pwc.com

Juan Pujadas*

1 646 471 7782

juan.pujadas@us.pwc.com

John S. Scheid*

1 646 471 5350

john.scheid@us.pwc.com

Andy Turner

44 20 7213 4988

andy.turner@uk.pwc.com

Hajime Yasui

81 3 5532 3041

hajime.yasui@jp.pwc.com

Specialist editorial contributions

Daniel A. DiFilippo

Partner, Global Risk Management Services

1 646 471 8426

dan.difilippo@us.pwc.com

Miles E. A. Everson

Partner, Financial Services – Finance, Operations, Risk and Compliance Solutions

1 646 471 8620

miles.everson@us.pwc.com

Charles Ilako

Lead Partner, European Financial Services

Regulatory Practice

32 2 710 71 21

charles.ilako@uk.pwc.com

Phil Rivett*

Global Leader, Banking and Capital Markets

44 20 7212 4686

phil.g.rivett@uk.pwc.com

* Member of the Global Financial Services Leadership Team

Compliance: A gap at the heart of risk management

Contacts *continued*



Global Financial Services Leadership Team

Jeremy Scott

Chairman, Global Financial
Services Leadership Team
44 20 7804 2304
jeremy.scott@uk.pwc.com

Etienne Boris

33 1 56 57 1029
etienne.boris@fr.pwc.com

Javier Casas Rúa

54 11 4891 4550
javier.casas.rua@ar.pwc.com

Rahoul Chowdry

61 2 8266 2741
rahoul.chowdry@au.pwc.com

Richard Stuart Collier

44 20 7212 3395
richard.stuart.collier@uk.pwc.com

Ian Dilks

44 20 7212 4658
ian.e.dilks@uk.pwc.com

Simon Jeffreys

44 20 7212 4786
simon.jeffreys@uk.pwc.com

John Masters

61 2 8266 7265
john.masters@au.pwc.com

Bob Moritz

1 646 471 8486
robert.moritz@us.pwc.com

Barry J. Myers

1 416 869 2441
barry.j.myers@ca.pwc.com

David Newton

44 20 7804 2039
david.newton@uk.pwc.com

Arno Pouw

31 20 568 7146
arno.pouw@nl.pwc.com

Juan Pujadas

1 646 471 7782
juan.pujadas@us.pwc.com

Rick Richardson

1 617 428 8333
rick.richardson@us.pwc.com

Phil Rivett

44 20 7212 4686
phil.g.rivett@uk.pwc.com

John S. Scheid

1 646 471 5350
john.scheid@us.pwc.com

Nigel Vooght

44 20 7213 3960
nigel.j.vooght@uk.pwc.com

Akira Yamate

81 3 5532 2518
akira.yamate@jp.pwc.com

Compliance: A gap at the heart of risk management

Contacts *continued*



Economist Intelligence Unit (EIU)

111 West 57th Street, New York, NY 10019

Andrew Palmer

44 20 7830 1149

andrewpalmer@eiu.com

Michael Kapoor

michaelkapoor@yahoo.com

For information on the PricewaterhouseCoopers Global Financial Services e-briefing programme please contact Áine O'Connor, Director, Head of Global Financial Services Marketing, on 44 20 7212 8839 or e-mail at aine.r.oconnor@uk.pwc.com

For additional copies please contact Alpa Patel at PricewaterhouseCoopers on 44 20 7212 5207 or e-mail at alpa.patel@uk.pwc.com