

Corporate Governance, Business Ethics, and Global Compliance Management

by Miles Everson, Charles Ilako, and Carlo di Florio

Financial services institutions are challenged as never before by failures of corporate governance and business conduct. Daily media coverage of financial institution complicity in the corporate failures plaguing Wall Street — along with other public concerns over money laundering, conflicts of interest, improper initial public offering allocations, and predatory lending, to name just a few — has heightened the scrutiny these institutions face from regulators. Reforms are reminiscent of those that followed the Great Depression, and there is a proliferation of proposals intended to restore trust, integrity, and responsibility in the financial services industry. Outside the United States, some major financial services institutions have run afoul of foreign regulations and found themselves sanctioned — sometimes severely.

Regulatory sanctions are bad; they cost time and money. The real damage, though, is to the firm's reputation, and potentially to that of the industry. In today's global financial markets, financial services institutions face ever more

This article looks at the links between corporate governance, business ethics, and compliance management. It assesses the current state of play and some of the leading practices in these areas. It puts forward some suggestions for designing an effective compliance function, and the implications with regard to corporate governance, business ethics, and organizational roles and responsibilities.

difficult challenges in protecting their reputations. To meet these challenges, they continually seek to improve the way they conduct their business and to manage their risks ever more effectively. Increasingly, it is recognized that corporate governance, ethics, and compliance practices are crucial guardians of a firm's reputation and integrity.

New challenges for the board and senior management

With continuing globalization of the financial markets — accelerated by technology, dramatic industry consolidation, and intensifying competition — regulators have reached the conclusion that certain issues need to be addressed on an international basis in order to protect the safety and stability of the financial system. Corporate governance and business conduct are high on the list.

Globally, regulators, investors, and other stakeholders increasingly hold the view that the business conduct and compliance function is a critical element of an organization's corporate governance structure. Corporate governance is not just about committee structures, stock options, and voting rights — it implies a comprehensive and consistent corporate commitment to integrity evident in its core values, leadership, culture, and business ethics.

The Basel Committee on Banking Supervision, International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS) have all released standards emphasizing management's responsibility to manage its business effectively. However, it is more than this. Regulators want management to *demonstrate* that it can



WESTBROOK

Recently compliance requirements have spread into previously unregulated sectors of the financial services industry as a result of money laundering and terrorist financing.

manage its business risks effectively and conduct its business ethically, across multiple jurisdictions, entities, products, and activities.

The issue of corporate governance has been the subject of much debate in Europe over the past few years. At the level of the European Union, the "Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe," issued in November 2002, has tabled a series of recommendations aimed at rationalizing EU company law to reinforce corporate governance.

In the United Kingdom there have been a number of corporate governance-related studies since the milestone Cadbury Report in 1992, culminating in the "Combined Code: Principles of Good Governance and Code of Best Practice" from the Committee on Corporate Governance. The Financial Services Authority (FSA) uses this code as a backdrop to its approach to senior manager responsibilities, to which a section of the FSA's new handbook is dedicated. As a result, the link between corporate governance and compliance becomes explicit. We expect that a similar clear link will be made in other European countries shortly, if it is not already.

In Germany a blue ribbon committee produced the country's first corporate governance code a year ago. In France, an extensive set of corporate governance rules was introduced in France as a result of the Viénot reports of July 1995 and July 1999. Nevertheless, in

light of recent events, a further review was recently completed by a working group chaired by Daniel Bouton, president of Société Générale, resulting in recommendations that are leading to fairly wide-reaching changes.

In the United States the recent wave of Wall Street scandals has resulted in widespread reform. Sarbanes-Oxley legislation is accompanied by active criminal and civil proceedings against financial services institutions, new rule making by the Securities and Exchange Commission and Government Accounting Office, revised listing and analyst standards (NYSE, NASD, AMEX, NASDAQ), new business practices for securities firms and rating agencies, and a host of new expectations and standards voiced by institutional investors, professional associations, and other stakeholders. Independence and disclosure are the prominent themes.

These reforms place new requirements on boards of directors, board committees, senior management, and key ethics and compliance functions. For boards, independence is required for the audit, nominating, and compensation committees. Boards are required to meet without management present, in "executive sessions." There are also a number of new compliance, code of conduct, and whistleblower protection requirements. The NYSE requires corporate governance and business ethics guidelines to be available on the institution's Web site. This, of course, requires that firms support such representations with substantive compliance processes

and practices to demonstrate meaningful commitment to business integrity.

Similarly, European regulators are now also strongly advocating the establishment of a global compliance function to support, coordinate, and monitor compliance activities at the business line, geographical, and legal-entity level. In a growing number of European countries, there are now explicit regulatory requirements covering these areas. For instance, global compliance coordination is necessitated by new requirements flowing from global efforts to combat corruption, money laundering, and terrorist financing.

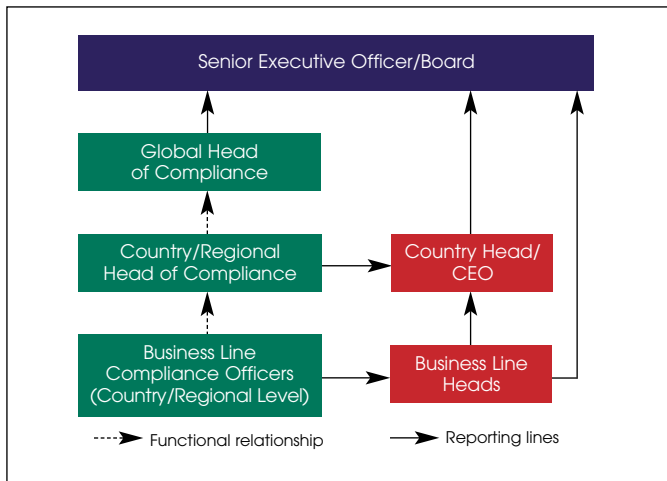
In effect, there is an interesting and significant development occurring in Europe. There are clear signs of convergence in the way European regulators are thinking, as evidenced not least by the work of the Committee of European Securities Regulators (CESR). The CESR recently issued standards for the harmonization of conduct of business rules in Europe, including a requirement to establish an independent compliance function. CESR members (the 15 member states of the European Union, plus Norway and Iceland) have made a binding commitment to either introduce these standards in their national jurisdictions (where they have the power to do so) or work to persuade legislators that such changes are necessary.

Current state of play

Compliance functions have their longest history in the United States, with much of the relevant legislation dating from the 1930s and 1940s. The regulatory requirements for compliance functions have expanded, at times gradually, and at other times, expansion has come in

Table 1: FSG criteria for an effective compliance program

Criterion	Indicative high-level self-assessment questions
1. Compliance standards and procedures	<ul style="list-style-type: none"> • Do comprehensive and consistent compliance policies and procedures exist throughout the enterprise? • Is the code of conduct a proactive and complete summary statement of the organization's positions on ethics and compliance?
2. High-level officer	<ul style="list-style-type: none"> • Have specific responsibilities for compliance been assigned to senior management and the board? • How are the reporting relationships for compliance structured to ensure independence and effectiveness?
3. Due care in delegating authority	<ul style="list-style-type: none"> • Are there appropriate and established limitations to signatory and decision-making power? • Is effective due diligence conducted on agents, consultants, and other business partners? • Does the organization conduct detailed performance monitoring for disciplinary action?
4. Effective communication	<ul style="list-style-type: none"> • Does the company conduct periodic compliance and awareness training for all employees? • Is training targeted for particular job responsibilities in compliance-sensitive areas?
5. Monitoring/auditing/reporting	<ul style="list-style-type: none"> • Is there a clear organizational chain of command for employees to approach for help with questions or reporting questions or concerns? • Does the company have a confidential means for employees to report concerns or ask questions about ethical issues anonymously (e.g., a helpline or confidential mailbox)?
6. Consistent discipline	<ul style="list-style-type: none"> • Has the company demonstrated willingness to reinforce compliance by consistently disciplining offenders, regardless of their position in the organization? • Is ethical behavior included as part of individual performance evaluations and as a predictor for successful advancement?
7. Process modification	<ul style="list-style-type: none"> • Does the company maintain records of compliance materials it has generated and revised, certification materials, and case handling records that may be needed in the event of future issues/investigations? • Does the company proactively monitor emerging issues and key risk areas to respond to real or potential problems and determine what remedial actions might be necessary?



concentrated bursts, as a reaction to scandals caused by rogue individuals or financial institutions, as a response to international events (e.g., the USA PATRIOT Act), or from a general updating of the U.S. financial system (e.g., the Gramm-Leach-Bliley Act).

More recently, compliance requirements have spread into previously unregulated sectors of the financial services industry (e.g., hedge funds, private equity funds, and venture capital firms) as a result of concerns about money laundering and terrorist financing.

Since 1991, compliance programs in the United States have been anchored, generally, in the framework established by the U.S. Federal Sentencing Guidelines (FSG) for Organizations. The FSG provides seven core criteria for managing a company's ethics and compliance risks (see Table 1, page 25).

Some comparisons can be drawn with Europe. PricewaterhouseCoopers has recently undertaken a study looking at the current state of play and future trends for compliance functions in Europe.¹ While compliance functions do not have the same history in Europe as in the

United States, the evolution of the compliance function over the past decade has been rapid. This evolution started from two different points of origin. In the United Kingdom, for example, the requirement for compliance functions grew out of market failures and focused primarily on

conduct of business rules. In other countries, where bank finance still remains the most prevalent form of financing, the need for a bank compliance function developed from the regulatory requirement for "adequate administrative and accounting organizations and systems of internal control." Now there is growing consensus across Europe that the compliance function should ensure regulatory compliance in all areas of the financial services institutions' operations. Starting from two different points of origin, the concepts are now converging quickly.

Globally, similar operational models are being adopted for the compliance function. The most prevalent model in the United States, and now in Europe, is a stand-alone compliance function. This reflects widespread recognition that the compliance function is an independent staff function supporting the governing and managing bodies that are ultimately responsible for compliance. To a greater extent than the internal audit function, the compliance function also needs to be close to business units on a day-to-day basis in order to spot potential compliance risks at the operational level and help resolving them.

A number of international banking and securities groups have established a centralized compliance function overlaying a network of local compliance officers who are based in front-line business units — thus addressing the need to be independent while staying close to business units. This approach responds well to business units' needs but can cause difficulties dealing with local regulatory requirements that center on legal entities. Other groups, therefore, have chosen to coordinate compliance activities both at the business line and country/legal-entity level. These approaches create potential difficulties in terms of both independence and consistency that warrant careful management attention. To operate effectively, a compliance function needs:

- a clearly defined structure and unambiguous reporting lines that preserve independence and demonstrate senior-level commitment;
- adequate financial and human resources — meaning, where possible, no direct reliance on business units for the necessary budgets and conflict-free human resources policies with regard to recruitment, remuneration, and performance assessments;
- a charter setting out roles and responsibilities and the scope of activities (covering in particular the interaction with other departments such as internal audit and legal);
- a realistic apportionment of responsibilities set forth in documented and monitored annual plans;
- periodic independent verification to assess program effectiveness and ongoing improvement.

Table 2: Best Practices for Achieving a Compliance-Supporting Culture

- Board and senior management commitment to ethics and compliance.
- Global compliance function supported by a cross-functional management compliance committee.
- Clearly defined objectives, success measures, and project management capabilities.
- Effective upstream and downstream communication.
- Consistent accountability at all levels.
- Integration of compliance into individual performance measurement and reward structures.
- Values-based approach to ethics and compliance.
- Knowledge management to facilitate learning and leverage successes and failures.
- Continuous improvement based on objective measurements.
- Effective use of compliance-enabling technology to enhance program management, communication, monitoring, and reporting
- Constructive engagement of internal and external stakeholders.
- Leveraging compliance process improvement to enable business process improvement.
- Systematic measurement of compliance program effectiveness, including managing and mitigating costs.
- Development of early warning systems and effective dispute resolution processes.
- Redefinition of the ethics and compliance program to encompass frameworks that provide support for corporate social responsibility (CSR) programs and triple bottom line reporting of the organization's economic, environmental, and social performance.

At the group level, care is needed to ensure consistent coverage — across business lines and geographies — with national requirements. One size does not necessarily fit all.

Leading practices

In the United States today many financial services institutions are looking to go beyond basic adherence to the FSG in terms of their compliance functions. Leading ethics and compliance programs seek not only to establish sound governance practices but also to embed compliance with such practices into corporate culture. Similarly, in Europe, it is increasingly recognized that the compliance function serves four key objectives:

- demonstrating compliance with relevant regulations;
- identifying, addressing, and resolving regulatory failures;
- managing the cost of compliance; and
- embedding compliance within the organization overall.

Currently, compliance functions in Europe often cope well with the first two but have yet to fully address the second two. The goal, nevertheless, is a corporate culture that both encourages and rewards compliance.

Embedding compliance

PwC has undertaken a considerable amount of work helping clients develop the essentials of a values-based compliance supporting culture. Through this, it has become clear that companies that have successfully evolved into leading

Table 3: Compliance Roles and Responsibilities

Enterprise Level

- Provide centralized compliance coordination and oversight with the support of the compliance committee.
- Set and communicate vision, objectives, and enterprise policies.
- Develop annual global compliance plans that link global and local objectives and goals.
- Ensure that compliance requirements encompass a full range of enterprise issues and objectives.
- Ensure that consistent policies are adopted across functions.
- Establish an umbrella plan for training and education.
- Help the enterprise achieve quality of service and product by participating in the new product/business line development process and assessing the compliance impact on existing business lines.
- Provide an ombudsman function to answer questions and address reported issues.
- Create a structure and protocol governing investigations.
- Provide tools and technologies for compliance assessment and implementation.
- Define key measurements to be used as a basis for program assessment and continuous improvement.
- Monitor enterprise and functional program performance.
- Create a structure and protocol to coordinate investigations and disciplinary actions.
- Provide coordinated knowledge management and facilitate sharing of best practices/lessons learned.
- Leverage the compliance framework for early issue identification and resolution.
- Identifying emerging issues and facilitate integration into business conduct framework.
- Report to management and the board on program performance, and develop effective compliance dashboard key performance indicators.
- Identify opportunities to leverage compliance process improvement to enable business process improvement.

Functional Support of Enterprise Program

- Implementation of enterprisewide framework in a manner that is consistent with and supports functional needs.
- Leverage enterprise tools and technologies to the extent practicable.
- Provide training and communication that are integrated into the enterprise umbrella framework.
- Monitor and measure program performance using established metrics.
- Identify emerging risks and develop proposed control frameworks.
- Report on program effectiveness (including incident management).
- Identify best practices and lessons learned for knowledge management and leverage at an enterprise level for continuous improvement.

practices in this area share several common traits that enable forward thinking, continuous improvement, and effective change management.

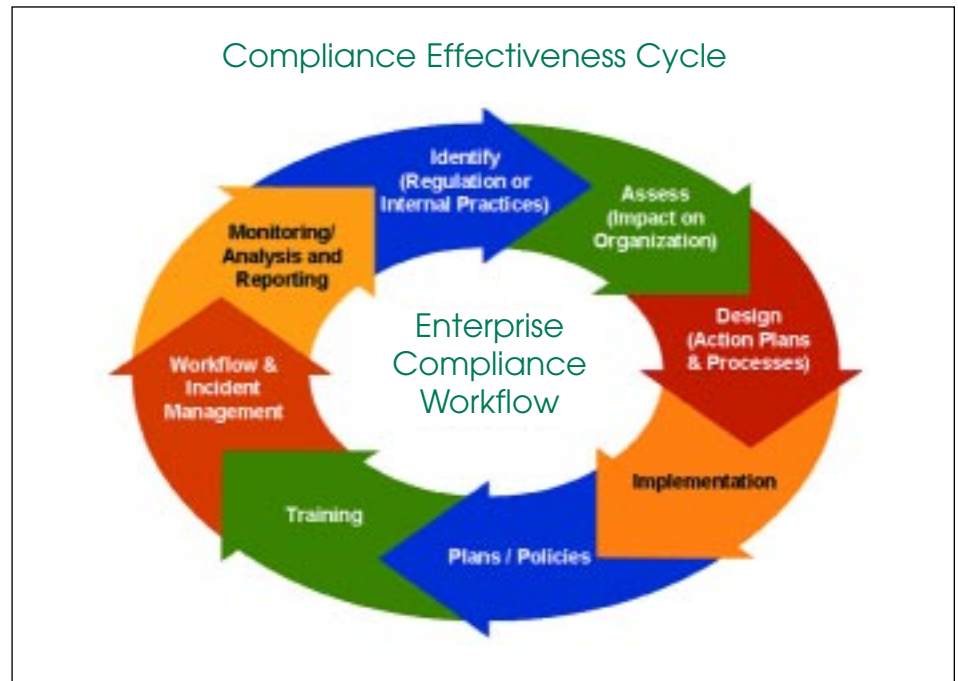
PwC has developed a broad-based approach to support clients in adopting companywide mandates to create a compliance-supporting cultures,³ called “total compliance continuum.” This approach focuses on cultivating an ongoing commitment to compliance throughout the organization and enables financial services institutions to build effective programs on three fronts:

1. *Through board and management “tone at the top.”* Business ethics address how a company cultivates a culture of doing the right thing and integrating core values, such as responsibility and trust, into the way business is conducted across the organization. Both the board and top management need a strong, unified vision concerning the compliance program’s purpose. Management is responsible for planning and implementing an effective compliance program, while the board oversees management to ensure that implementation occurs and corporate responsibilities are met on an ongoing basis.

2. *Through a values-driven code of conduct.* Values serve as a beacon for a company’s decision-making processes and determine how a company behaves in uncertain times. The company’s ethics and values regarding compliance need to be “lived” and embodied in a clearly written code of conduct that is meaningfully communicated to all employees and associated third parties. This code should not only express management’s values but also identify and reflect the values of major stakeholders.

3. Through effective integration in business processes. Integration with business processes includes developing clear policies and procedures; communicating to, and training, employees about the code of conduct and related practices; monitoring progress; reporting to management and the board; fine-tuning strategies; and communicating the company's successful performance to key stakeholders. Integration ensures that the compliance and ethics program becomes operational and effective.

When designing a compliance function, an institution must consider both functional roles and compliance responsibilities, together with enabling technologies and emerging standards



Examples of Key Performance Indicators

- Board/senior management oversight practices and charters
- Code of conduct awareness and signatures
- Ethical culture surveys of employee opinions
- Helpline awareness and call resolution
- Compliance process effectiveness ratings
- Training records and effectiveness
- Adequacy of program documentation
- Awareness of newsletters and articles
- Risk management and early detection
- Consistency of enforcement
- Management response to issues raised
- Management response to audit findings
- Helpline trends
- Degree of ethics message integration
- Percentage of questions versus allegations
- Investigation results
- Exception reporting (e.g., know your customer checks, fact-finding quality, market transactions)
- New account openings and business volumes by product and customer type
- Number of sales observations conducted
- Appraisals and observations outstanding

that subsequently should be incorporated in the compliance program.

Key success factors

The “good” compliance officer has come a long way from the “You can’t do that” school to one in which he or she is more than prepared to give advice and assistance to all areas of the business. This has been described by one compliance officer as “the art of the possible” — helping the firm understand what *can* be done from a regulatory viewpoint, coaching on best practice, passing on lessons learned outside the firm (and even outside the industry), acting as a sounding board, and in general showing management that getting the customer’s experience right from a commercially driven viewpoint can also meet key governance, compliance, and regulatory requirements. To achieve this balance in the compliance department, leadership,

vision, creativity, proactivity, and outstanding communication skills are necessary.

A key issue is staffing. The staffing of either the head office compliance unit or the regional/local office compliance unit (or individual) will depend upon numerous factors, including the following:

- overall staffing of the financial services firm;
- the types of customers served by the institution (retail and/or institutional);
- the products offered to the customer base (e.g., commercial and/or consumer lending, money markets, capital markets, whether primary offerings and/or secondary trading);
- the geographic reach of the company (local, regional, national, or international); and
- the various distribution channels used by the institution (e.g., sales

forces, third-party marketers, bricks and mortar offices, and cyberspace).

The mixture of the above factors, plus others (for example, the local governance and regulatory environment at each international office, its specific rules and complexities, and the application of technology in the compliance process) will affect the level of compliance staff required, as well as the competencies and experiences of the staff utilized, in order to enforce and monitor the applicable standards, rules, and regulations the financial services institution must follow.

While the chief compliance officer of an organization will usually have a broad compliance background, the exact experience of the unit's staff and its applicability to various front-office departments and products has become an increasingly important factor. Just having a compliance unit is not enough; the staff must have the requisite competencies and specialties in order to master compliance risk and understand

the ways in which it manifests itself at the group, entity, business unit, product, and transaction levels.

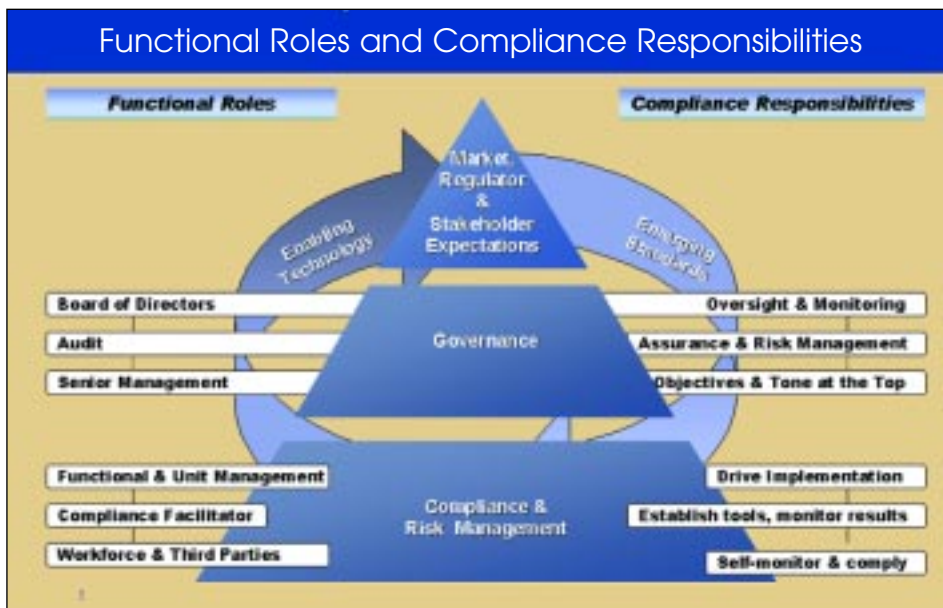
Performance monitoring

Compliance functions and programs should be independently reviewed on an annual basis, by internal audit and possibly by external parties to assess effectiveness. Across the financial services industry, compliance functions have developed a wide range of compliance dashboards to help them assess program effectiveness and monitor the compliance risk profile of the business on an ongoing basis.³

Although these dashboards vary in terms of their content, sophistication, and presentation style, they have a common feature: feedback to management and the board regarding a number of prescribed key performance indicators (KPIs) — a fundamental of good corporate governance.

From work in this area, PwC has learned a number of lessons relating to the use and effectiveness of compliance metrics and dashboards:

The first lesson is that the most effective dashboards do not concentrate solely on the purely compliance-related KPIs (such as persistency), but also include some reference to the broader business performance of the organization, such as sales performance, and training and competence statistics. This provides management with a much broader view of the organization's compliance performance, and allows for more immediate identification of the underlying issues that may be causing the poor compliance performance.



The second lesson is that the dashboard should be devised in such a way that it enables the cross-referral of KPIs and makes for easy identification of correlations. An obvious example might be the possible correlation between the average span of control and the number of sales observations outstanding. However, we have seen instances where correlations have been identified between two KPIs that would not at first glance seem connected but which, on investigation and over time, have proved to be linked and of significance. The dashboard must show the KPIs as trends and not just as one-off figures. What is of interest to management is the ways in which the KPIs change over time and not just the absolute figures.

Finally, there is a feature of compliance dashboards that we have not yet seen, but which we expect to see developed and have discussed with clients. Hitherto, dashboards have traditionally been historical; they report what has happened in the recent past. If dashboards contain the trend and correlation analysis capabilities described above, we see no reason why they cannot become a tool for use in planning the future. By extrapolating trends, and by using as predictive tools the correlations already identified, it should, in our view, be possible to use the dashboard as a tool for scenario planning and impact assessment. This would enable the compliance officer to more effectively fulfill his or her role as a strategic adviser: The dashboard would give him or her the means to say to management “if you do this, that will happen”; he or she would be able to show the cause-and-effect linkages between the various factors involved in running a regulated firm.

Compliance-enabling technologies

Compliance departments in U.S. financial services institutions use a variety of additional tools — such as robust risk management frameworks, early issue identification and resolution processes, and balanced scorecards — that drive ethics and compliance performance throughout the organization.

Knowledge management is improving, generally, in compliance departments with the use of internal bulletin boards, intranets, and knowledge databases. The more sophisticated tools allow firms to track issues and breaches and keep affected parties informed of their resolution. Specifically, the use of data mining systems to enhance monitoring for anti-money laundering purposes has acquired increased importance after the events of September 11. Such systems are already widely used in the United States and their use is increasing in Europe. These systems have proved to be highly effective for comparing actual customer transactions against a customer’s profile. They have enormous potential for monitoring compliance with conduct of business requirements that impose a duty of care on a financial services institution.

A host of new compliance-enabling technologies are emerging that provide enterprisewide compliance solutions, as opposed to more traditional solutions that address specific issues, such as money laundering. These new enterprise solutions provide knowledge management for all the compliance policies and procedures of an organization; facilitate the compliance management processes; allow the firm to communicate, train, track, test, and verify awareness and understanding

among employees; and pipe into transaction systems using rules-based engines to identify and elevate risks and trigger workflows.

In effect, compliance departments must retool and reskill themselves with new frameworks and methodologies for risk assessment and they must obtain enhanced management information to measure and monitor compliance. They will need to make better use of new technology if they are to report on and demonstrate compliance to senior management, boards of directors, regulators, investors, and other key stakeholders. In making these changes, they must ensure that they are properly aligned with their firms’ business strategies, operational business, and the expectations of major stakeholders.

The Value

Corporate governance, business ethics, and effective compliance management are increasingly critical to financial services institutions. Globalization, technology, and product complexity present challenges across the board. For the financial services industry, however, these are compounded by regulators’ concerns about business conduct, money laundering, conflicts of interest, predatory lending, improper marketing and many other business integrity issues. To safeguard one’s reputation, the best way forward is to embed ethics and compliance into all systems, processes, and procedures — basically into the culture of the organization.

However, embedding ethics and compliance into corporate culture could be a major challenge. The roles and responsibilities of the board and senior management, in addition to those of

the compliance function, need to be extremely clear. The organization and structure of the compliance function, reporting lines and review processes, the required skills and competencies of compliance personnel, the use of enabling technologies, and, not least, the key performance indicators that will be used to measure the effectiveness of the compliance function all need to be considered carefully. But this is only part of the picture. Embedding compliance will require cultural change — the impact of which will differ from organization to organization. The key challenges for management will be, first, to design, communicate, and operationalize effective governance, values, and compliance throughout the organization. In today's environment, a firm's success or failure may well rest on the manner in which it effectively and holistically addresses corporate responsibility. ❖

about the authors

Miles Everson is a partner with PricewaterhouseCoopers in New York, focusing on operational effectiveness in the financial services industry.

Charles Ilako is a partner with PricewaterhouseCoopers in London and leads the financial services regulatory advisory practice in Europe, the Middle East, and Africa. **Carlo di Florio** is a director with PricewaterhouseCoopers in New York, focusing on corporate governance, business ethics, and compliance management solutions. The authors can be reached at (646) 471-4000.

This article draws on extensive PricewaterhouseCoopers' thought leadership in the area of corporate governance, business ethics and compliance management. Special appreciation goes to Bob Bench and Roger Coffin in the United States, Andrew Podd in the United Kingdom, Peter PT Li in Hong Kong, and Wendy Reed in Belgium.

Have a question or comment?

Use the postage-paid reply card provided in this issue or leave a message at (202) 663-5075.

1. "Regulatory Compliance: Adding Value. A Review of Future Trends," October 2002.
2. "Corporate Governance - Compliance at the Core."
3. "Best Practice and Delivering Value — The Future for Compliance."