Susan Schmidt Bies: Enterprise-wide compliance programs

Speech by Ms Susan Schmidt Bies, Member of the Board of Governors of the US Federal Reserve System, at the Bond Market Association's Legal and Compliance Conference, New York, 4 February 2004.

* * *

Introduction

I want to thank the Bond Market Association for the opportunity to speak to you this afternoon. Given the evolution of the financial markets and financial services industry and the unfortunate events that some firms have recently encountered, comprehensive and robust management of legal and reputational risks is becoming more essential. The agenda for this conference reflects many of the concerns that have been raised over the past two years regarding legal and reputational risks in general, and conflicts of interest, the adequacy of public disclosures, and the transparency of accounting in particular.

I know that we all hoped that with the new year we could put behind us the corporate governance shortcomings and financial restatements of the past several quarters. Unfortunately, the news about Parmalat demonstrates that we are not yet out of the woods and that corporate governance problems are not limited to the United States, but are a global issue. Financial firms are facing losses and possible legal and reputational risks in connection with their dealings with this company. The industry still has a lot of work to do in managing risks, and this conference is an excellent step toward addressing important risk-management issues in the context of the compliance function.

In addition to sponsoring this timely conference, the Bond Market Association has been at the forefront of myriad initiatives relating to risk management and compliance. One especially important initiative has been the association's participation with other industry groups in establishing the Joint Market Practices Forum. The forum's first initiative has been to articulate a statement of principles regarding the handling and use of material, nonpublic information by credit market participants. The statement of principles fulfills a number of objectives. The most critical, in my view, is the promotion of fair and competitive markets in which inappropriate use of material, nonpublic information is not tolerated. At the same time, the statement allows lenders to effectively manage credit-portfolio activities to facilitate borrower access to more-liquid and more-efficient sources of credit. This recognizes that the liquidity and efficiency of our financial markets are related directly to the integrity of, and public confidence in, those markets.

The forum's statement of principles also provides a number of meaningful recommendations, some of which have already been adopted by the major participants in the credit derivatives market. The statement and recommendations have sparked much-needed discussion and helped identify issues, such as conflicts of interest and insider trading, that may arise in connection with credit portfolio management. These are important steps toward improving the risk-management environment, and I commend you for voluntarily taking the initiative.

One aspect of the forum's statement that I would particularly like to applaud is its focus on controls and compliance across the consolidated organization, because that focus ties directly to my remarks today. Specifically, I would like to discuss the need for financial services firms to develop enterprise-wide compliance programs for legal and reputational risk management. As financial firms continue to grow more complex and add new products, services, and activities - all of which are natural and positive market developments - they need to have a process to facilitate the evolution of the culture of compliance across the organization.

I am first going to discuss the importance of an enterprise-wide approach to risk management and identify some particular areas in which an integrated approach can improve internal controls. Then I will talk about how compliance and internal audit can foster effective risk management.

Enterprise-wide risk-management framework

What do I mean by an enterprise-wide compliance program? I would define it as an integral part of an overall risk-management framework that is adopted by an entity's board of directors and senior management and is applied in setting a strategy throughout a firm. As you may know, the Committee

of Sponsoring Organizations of the Treadway Commission, or COSO, is in the process of finalizing an enterprise-wide risk-management framework that is expected to be published later this year. The principles the new COSO document espouses transcend functional areas, and I expect that it will be an important contribution to the ongoing discussion of how risk management can be strengthened across different types of organizations and functional areas.

For those of you not familiar with the COSO framework, let me briefly explain that an enterprise-wide risk-management framework identifies potential events that may affect the entity and establishes how the organization will manage its risk given the firm's risk appetite and strategic direction. In an enterprise-wide risk-management framework, managers are expected to evaluate at least annually the risks and controls within their scope of authority and to report the results of this process to the chief risk officer and the audit committee of the board of directors.

In evaluating risks, managers need to consider both current and planned or anticipated operational and market changes and identify the risks arising from those changes. Once risks have been identified comprehensively, assessed, and evaluated as to their potential impact on the organization, management must determine the effectiveness of existing controls and develop and implement additional appropriate mitigating controls where needed.

The robustness and effectiveness of these controls must be evaluated independently, soon after the control structure is established, so that any shortcomings can be identified promptly and corrected. Risk assessments initiated early in the planning process can give the firm time to implement mitigating controls and conduct a validation of the quality of those controls *before* launching the product. Strong internal controls and governance require that these assessments be done by an independent group. One of the weaknesses that we have seen is that management delegates both the development and the assessment of the internal control structure to the same risk-management, internal audit, compliance, or legal division. Instead, it is important to emphasize that line management has the responsibility for identifying risks and ensuring that the mitigating controls are effective, and that the assessments should be done by a group independent of that line organization.

An enterprise-wide approach also can integrate the risk assessment of functions that have traditionally been managed in "silos". Conflicts can arise in many different areas and functions of the firm, including sales and research. Conflicts can also occur when compensation structures create incentives inconsistent with prudent risk management or when the bottom line for the current quarter is unduly emphasized without adequate consideration of the risk being taken to accomplish those results. The potential for these conflicts to arise must be addressed squarely by senior management, and appropriate controls must be in place to manage and mitigate conflicts.

A culture of compliance should establish - from the top of the organization - the proper ethical tone that will govern the conduct of business. In many instances, senior management must move from thinking about compliance chiefly as a cost center to considering the benefits of compliance in protecting against legal and reputational risks that can have an impact on the bottom line. It is important to note that the board of directors and senior management of financial firms are responsible for setting the "tone at the top" and developing the compliance culture that has been discussed at this conference. The board and senior management are obligated to deliver a strong message to others in the firm about the importance of integrity, compliance with the law, and overall good business ethics. They also need to demonstrate their commitment through their individual conduct and their response to control failures. The message and corresponding conduct should empower line staff to elevate ethical or reputational concerns to appropriate levels of management without fear of retribution.

Reputational and legal risks pose major threats to financial services firms because the nature of their business requires maintaining the confidence of customers, creditors, and the general marketplace. Importantly, legal and reputational risk can negatively affect the profitability, and ultimately the viability, of a financial firm.

Enterprise-wide compliance program

A strong compliance program is an integral part of the risk-management function. For the reasons I will discuss, the best practice in complex financial firms is to conduct risk management on an enterprise-wide basis. As a result, compliance activities should be managed on an enterprise-wide basis as well.

Traditional risk management has focused on quantifiable risks, such as credit and market risks. Recent events have demonstrated the need for greater focus on the risks that are harder to quantify -

that is, operational, legal, and reputational risks. Indeed, legal and reputational risks are significant risks facing some financial firms today. The compliance area is critically important in identifying, evaluating, and addressing legal and reputational risks. Given the significance of these risks, a strong enterprise-wide compliance program is a necessity for complex financial firms. A well-executed compliance program can also highlight operational problems.

As an integral part of an enterprise-wide risk management, an enterprise-wide compliance program looks at and across business lines and activities of the organization as a whole to consider how activities in one area of the firm may affect the legal and reputational risks of other business lines and the enterprise as a whole. It considers how compliance with laws, regulations, and internal policies, procedures, and controls should be enhanced or changed in response. This approach is in marked contrast to the silo approach to compliance, which considers the legal and reputational risks of activities or business lines in isolation without considering how those risks interrelate and affect other business lines. The silo approach to compliance has prevailed for far too long in financial firms. We are overdue for a paradigm shift to an enterprise-wide compliance structure as we also shift to enterprise-wide risk management.

Why is an enterprise-wide compliance program so important? Recently, in an interview with *The Wall Street Journal*, the independent board chairman of a prominent mutual fund company involved in the market-timing scandal identified as one of the firm's compliance breakdowns the bifurcation of compliance responsibilities within the firm. That is, no one had the 25,000-foot view of what was happening across the organization, and this led to internal control shortcomings that were not identified and to opportunities for employees to take unfair advantage of other market participants. Moreover, the compliance function did not have the status and perceived importance it should have had. The company's board reportedly has installed a board-level compliance officer in response to a review of the circumstances surrounding the control deficiencies. This addition helps to ensure that the board, the group that is ultimately responsible for risk management, can assess the quality and robustness of compliance across the organization.

Enterprise-wide compliance programs incorporate controls that include transaction approval and monitoring procedures in all relevant functional areas. They also provide all decisionmakers with complete and comprehensive information about the proposed transaction. Involving all relevant functional areas and decisionmakers allows for an enhanced review of a transaction, one that considers the impact of the transaction across the consolidated organization. As a result, compliance is conducted on a comprehensive, holistic basis and not in silos. Involving all functional areas and decisionmakers also focuses attention on all the relationships a client may have across the organization, allowing identification of conflicts of interest or other sources of legal and reputational risks.

Viewing compliance across the organization's different functions minimizes the potential for legal and reputational risks to be overlooked. As a result, compliance policies, procedures, and controls are less likely to be inadequate. For example, conflict-of-interest policies and controls may be inadequate if risk management in the traditional credit function does not also consider the activities being conducted in the trading and sales areas.

An enterprise-wide compliance program helps management and the board understand where the legal and reputational risks in the organization are concentrated, provides comparisons of the level and changing nature of risks, and identifies those control processes that most need enhancement. This process, in turn, can facilitate analysis of whether the legal and reputational risks taken in a particular part of the organization are appropriate. Of course, the ability to assess legal and reputational risks across the enterprise depends heavily on the quality and timeliness of information. The compliance function must ensure that controls and procedures capture the appropriate information to allow senior management and the board to better perform their risk management functions.

The enterprise-wide compliance function should look at what is being reported to the board, the audit committee, and senior management regarding new or changed processes, procedures, and controls. Is there an effective mechanism for reporting control failures or limit exceptions? How are these exceptions pursued for follow-up action, and how are corrective actions communicated back to the board or management? Importantly, the compliance function should have a direct line to the general counsel through which it can report concerns and needed improvements to processes and controls.

The focus on an enterprise-wide approach to compliance does not mean that the organization cannot leverage off of specific business-line compliance functions. Indeed, it is very important to retain business-line compliance functions because they are staffed by individuals who understand the

activities being conducted and know where control breakdowns have occurred in the past. For example, the compliance function for a trading operation requires staff with detailed understanding of the back office, the middle office, and the front office. The enterprise-wide compliance approach supplements this business-line-specific view of compliance with a big-picture approach at the corporate level that encompasses and has access to all lines of business and operational areas. It incorporates the various business-line compliance reviews in assessing the robustness and adequacy of enterprise-wide legal and reputational risk management, and it ensures that significant issues are brought to the attention of senior global compliance officers as appropriate.

The enterprise-wide view is particularly important when functions cross business lines and management lines of responsibility. When business lines or managers share responsibility for compliance, specific duties and chains of accountability need to be established at the line-management level and overseen by the person ultimately responsible for compliance across the organization.

An enterprise-wide compliance program is also dynamic, constantly assessing new legal and reputational risks when new business lines or activities are added or existing activities are altered. Constant reassessment of risks and controls and communication with the business lines is necessary to avoid a compliance program that is operating on autopilot and does not proactively respond to change in the organization.

The role of the new-product approval process

The compliance program is an important participant in the new-product approval process, along with other relevant parties, including credit risk, market risk, operations, accounting, legal, audit, and senior line management. Compliance personnel should have an active voice in determining whether a particular activity or product constitutes a new product requiring review and approval. New products include products or services being offered to, or activities being conducted for the first time in, a new market or to a new category of customers or counterparties. For example, a product traditionally marketed to institutional customers that is being rolled out to retail customers (hedge funds, for instance) generally should be reviewed as a new product. In addition, significant modifications to products, services, and activities or their pricing warrant review as a new product. Even small changes in the terms of products or the scope of services or activities can greatly alter their risk profiles and justify review as a new product. When in doubt about whether a product, service, or activity warrants review as a new product, financial firms should err on the side of conservatism and route the proposal through the new-product approval process. Cutting short a new-product review because of a rush to deliver a new product to market, or because of performance pressures, increases the potential for serious legal and reputational risk.

The determination of whether a new or modified activity requires additional compliance processes, procedures, or controls is clearly the province of the compliance staff. It involves the interaction of business-line compliance staff with personnel responsible for enterprise-wide risk management. Once these processes, procedures, or controls are designed, compliance personnel should help ensure that those controls are implemented effectively and are a comprehensive response to the legal and reputational risks posed.

The role of internal audit

Just as the compliance area performs an independent review of the firm's activities and business lines, the compliance program also needs to be reviewed independently. Internal audit has the responsibility to review the enterprise-wide compliance program to determine if it is accomplishing the firm's stated objectives, and if it is adequately and appropriately staffed, in light of growth, changes in the firm's business mix, new customers, strategic initiatives, reorganizations, and process changes. Internal audit should evaluate the firm's adherence to its own compliance and control processes and assess the adequacy of those processes in light of the complexity and legal and reputational risk profile of the organization.

It should be obvious that internal audit, like the compliance program, needs to be staffed with personnel who have the necessary skills and experience to report on compliance with financial institution policies and procedures. Internal audit should test transactions to validate that business

lines are complying with the firm's standards and report the results of that testing to the board or audit committee, as appropriate.

Structured transactions

There are "lessons learned" from the legal and reputational risks that some financial firms faced in structuring transactions for Enron and WorldCom, among others. Those legal and reputational risks require a focus on appropriateness assessments, the enforceability of netting and collateral agreements, undocumented customer assurances, insurance considerations, and potential IRS challenges.

Assessments of the appropriateness of a transaction for a client traditionally have required firms to determine if the transaction is consistent with the financial sophistication, financial condition, and investment policies of the customer. Given recent events, it is appropriate to raise the bar on appropriateness assessments in the approval process for complex structured transactions by taking into account the business purpose and economic substance of the transaction.

When firms provide advice on, arrange, or actively participate in a complex structured finance transaction, they may assume legal and reputational risks if the end-user enters into the transaction for improper purposes. Firms should have effective and consistent policies and procedures that require a thorough review of the business purposes and economic substance of the transaction by all relevant functional areas and an assessment of any legal or reputational risks posed by the transaction. In instances that present heightened legal or reputational risk, the policies and procedures should require a review, by appropriate senior management, of the customer's business relationship with the firm. Of course, these policies and procedures need to be supported and enforced by a strong tone at the top and a firm-wide culture of compliance.

Conclusion

The evolution of the financial markets and the number of significant governance issues recently faced by complex financial firms clearly underscore the need to view risk management on an enterprise-wide basis. An integral part of a robust legal and reputational risk-management function is a strong compliance program. For such programs to be effective in complex financial institutions, compliance must be addressed on an enterprise-wide basis.