Mark W Olson: Compliance risk management in a diversified environment

Remarks by Mr Mark W Olson, Member of the Board of Governors of the US Federal Reserve System, to the Financial Services Roundtable and the Morin Center for Banking and Financial Services, Washington, DC, 16 May 2006.

* * *

Thank you for the opportunity to share my perspective on effective compliance risk management for diversified financial institutions. This area of risk management has been receiving a good deal of attention lately. Risk, to state the obvious, is inherent in all activities in the financial services industry. Because the industry is heavily regulated, compliance risk is an important element of the activities in which you are engaged.

Today, the financial services industry is experiencing tremendous growth, diversification, and innovation. This growth should be embraced as we consider the future of our financial sector. However, our "embrace" should be in the form of a sound risk-management framework. My remarks today will focus on what Federal Reserve supervisors see as the key components of a sound and effective compliance-risk management framework.

Before I begin, let me clarify what I mean by "compliance risk." Compliance risk can be defined as the risk of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value that arises when a banking organization fails to comply with laws, regulations, or the standards or codes of conduct of self-regulatory organizations applicable to the banking organization's business activities and functions.

A consolidated--or "enterprise-wide"--approach to compliance risk management has become "mission critical" for large, complex banking organizations, for several reasons. First, because compliance failures have touched many businesses, including banking, securities, and insurance firms, it has become clear that companies operating in more than one type of business must have a compliance strategy that is both globally consistent and locally effective. Increasingly, large, complex organizations are taking an enterprise-wide compliance-risk management approach to augment and better coordinate what had been fragmented and duplicative compliance activities. Such an approach puts local compliance activities within individual business lines into an integrated, global program, makes possible an understanding of compliance requirements and performance across an organization, and promotes consistency in responsibility, expectations, documentation, assessment, and reporting. I have been told that this more-integrated approach to compliance risk management by industry is already having a positive effect on risk identification and mitigation.

Second, the need for an enterprise-wide approach to compliance risk management at larger, more complex firms is suggested by the diversity of laws and regulations that span business lines, legal entities, and geographic boundaries--for example, in the areas of Bank Secrecy Act compliance and anti-money laundering controls, fair lending, information security, privacy, transactions with affiliates (Regulation W), and conflicts of interest. A more-integrated approach may be warranted for other matters, as well, because similar laws and regulations exist across the various jurisdictions in which the organization operates, both in the United States and overseas.

Because of the nature and levels of risks inherent to their business activities, complex banking organizations should have in place a compliance-risk management framework that makes it possible to identify, monitor, and effectively control the compliance risks facing their entire organization. Of course, such a framework needs to be commensurate with the nature and level of the organization's compliance risk. It should evolve with the ever-changing product lines and business activities of any growth-oriented organization. And, of course, it needs to stay on top of regulatory developments.

Setting the tone at the top--the role of the board of directors

A successful compliance-risk management program starts at the top of the organization. It is essential that the board of directors take the lead by requiring a top-to-bottom compliance culture that is well-communicated and incorporated into the organization's day-to-day operations by senior management, in order to ensure that all staff members understand their compliance responsibilities and their roles in implementing the enterprise-wide program. A strong compliance culture is evidenced by the extent to

which employees work together both to raise concerns about compliance risks and to design and establish effective controls.

A sound and effective enterprise-wide compliance-risk management program has strong board and senior management oversight. However, it is important to note that the board of directors and senior management have distinct, though complementary, roles in ensuring the program's success. As I mentioned, the board of directors is responsible for requiring a strong compliance culture. This environment should assure that compliance is an integral part of day-to-day operations. To this end, the board should approve the key elements of the program and then entrust responsibility for embedding the culture and implementing the program to managers and staff at all levels of the organization. Periodically, the board should be apprised of the extent to which predetermined benchmarks are being met.

Many of the largest and most complex banking organizations have established a corporate-level function to oversee their enterprise-wide compliance-risk management program, and the Federal Reserve views this trend very favorably. In these cases, the central function has been staffed with experienced compliance officers who are able to provide substantive guidance to business line managers and to keep senior management and boards of directors informed on how well the program is functioning, including by alerting them promptly about any material compliance breaches. Overall, such a central function can contribute a great deal toward ensuring that the key elements of a sound and effective compliance-risk management program are present and functioning as intended.

Corporate standards--tailored within the business lines

How does a board-mandated "compliance culture" permeate a banking organization? Among other ways, the culture and expectations are communicated through enterprise-wide compliance-risk management standards or objectives--established by senior management within a corporate-level compliance function--that reflect the expectations of the board.

Regardless of the compliance-risk management framework employed, the business line managers continue to "own" the compliance risk. That is, they are responsible for achieving compliance in their business lines and suffer the consequences in the event of compliance failures or missteps. Business line managers convert the corporate compliance risk standards or objectives into policies and procedures tailored to the specific type and level of compliance risk inherent in their activities and to the specific laws of the jurisdictions in which they operate.

To create appropriate compliance risk controls, organizations seek first to understand compliance risk across the entire entity. Managers assess and evaluate the risks and controls within their scope of authority at least annually. However, an enterprise-wide compliance-risk management program is dynamic and proactive, meaning that risks are assessed whenever new business lines or activities are added or existing activities and processes are altered. Once a particular business line has identified and assessed its compliance risks, it can design policies, detailed day-to-day procedures and processes, and associated risk-mitigating internal controls. The corporate compliance function plays an important role in advising business line managers as they assess risk. Such counsel adds to consistency in approach and helps control for mis-estimated risk. The corporate compliance function's involvement also increases the organization's ability to aggregate and better understand risks across the organization. Understanding of risk helps both the business lines and the compliance function develop internal controls that are reasonably designed to mitigate the risk.

While the industry trend toward more-consolidated compliance risk management is a favorable development, it is critical that business line management remain engaged. As I noted, senior managers in the business lines remain the "owners" of the risk, and compliance risk mitigation must be integrated into their overall business processes. The sense of ownership can be reinforced by factoring compliance ratings into performance measures and rewards. I am aware that, increasingly, organizations are tying compensation to management's ability to maintain strong internal controls and compliance processes. This practice helps keep the organization focused on managing compliance risk. To ensure that issues are escalated as they arise, the compliance staff embedded within the business lines should be independent and should have a clear reporting relationship to the corporate compliance-risk management function. In addition, to be most effective, the business line compliance staff should be "right-sized" to the level of risk within that business line.

Clear lines of reporting, authority, and communication are key to the success of any compliance-risk management framework. Policies and procedures should spell out for business line staff how to

escalate compliance concerns, should delineate responsibilities (avoiding overlapping roles and conflicts of interest), and should ultimately ensure that the board and senior management are fully apprised of material compliance events.

Monitoring and reporting

As I mentioned at the start, the fundamental purpose of the enterprise-wide compliance-risk management framework is to identify, monitor, and manage compliance risk more effectively. Among other things, monitoring is the means of identifying and communicating compliance breaches to the appropriate points within the organization. Banking organizations are establishing processes for monitoring the implementation of compliance policies, procedures, and controls, at both the consolidated and business line levels.

Sound compliance-risk monitoring activities at large, complex banking organizations are supported by information systems that provide management with timely reports related to compliance with laws and regulations at the transaction level. These reports generally address monitoring and testing activities, actual or potential material compliance deficiencies or breaches, and new or changing compliance requirements. Reports such as these ensure that information on compliance is communicated to the appropriate levels within the organization. Monitoring and reporting enable senior management and the board to effectively carry out their respective responsibilities.

At the frontier of compliance risk monitoring, larger, more complex banking organizations are moving toward the collection and analysis of quantitative information relating to compliance risk activities at the transaction level. Bearing in mind that this is an evolving area, banking organizations are investing in the development and application of such information as key risk indicators and key performance indicators in order to facilitate more accurate and more timely monitoring. Increased development and use of key compliance risk and performance indicators will ultimately enable better measurement, monitoring, and control of compliance risk.

Testing

As with other control functions within an organization, independent testing should be conducted to verify that compliance-risk mitigation activities, including training and internal controls, are in place and functioning as intended throughout the organization. Whereas monitoring is an ongoing process, testing is a "point-in-time" event, a critical check of performance. The frequency of testing should be based on risk--on such factors as whether significant deficiencies were identified through a recent examination or during the last testing; whether the business line's products or activities have grown or changed significantly; or whether a high risk that may directly affect the organization's activities has been identified.

Exceptions to the corporate-wide risk standards or objectives are reported to senior management, and I understand that this is most effectively done through reporting channels not under the direct control of business line management; however, resolution of the exceptions is the responsibility of business line management. An exception is tracked until its resolution has been validated. Importantly, a sound testing program contains provisions for escalating unresolved exceptions to higher levels in the organization, including the board of directors. Of course, the program should clearly define and communicate the roles of the internal audit, compliance, and other independent functions or third parties, although these roles will vary by organization.

Testing provides important feedback on how well the internal control framework is operating in practice, pointing the way toward any remedial actions that need to be taken. This essential part of an internal control framework can be performed by compliance personnel, audit personnel, or third-party firms that have specialized expertise. While banking organizations sometimes outsource compliance testing or other compliance function tasks, the organization itself remains accountable and must exercise appropriate oversight.

The "war for talent"

We've heard industry leaders refer to their compliance recruitment process as a "war for talent." Running an effective enterprise-wide compliance-risk management program requires more than

policies, procedures, and management information systems. Decisions are made by senior management on the basis of advice from their staff. Consequently, talent is required at all levels. In assessing the risk management of individual organizations, we have noted the importance of staff who have experience and expertise consistent with the scope and complexity of an organization's business activities. Staff must also have the integrity, ethical values, and competence consistent with a prudent management philosophy and operating style. We understand that hiring and retaining qualified and experienced compliance staff is a key challenge across the industry. Successful organizations are focusing not only on recruiting talent, but also on developing staff from within. Training and other staff-development tools are essential in this time of "war for compliance talent."

The role of the regulators

The business lines and activities of financial services firms can cross the jurisdictional boundaries of many legal entities, making it more difficult for a supervisory agency acting alone to determine what went wrong and what processes may need to be improved. In these cases, the Federal Reserve, as the consolidated supervisor of the banking organization in question, works closely with the primary bank regulator and the Securities and Exchange Commission (SEC) to investigate control breakdowns. The agencies exchange information and compare their findings. For example, findings from SEC examinations of broker-dealers, investment advisers, and mutual fund distributors are analyzed together with findings from targeted joint reviews of bank holding companies and banks conducted by the Federal Reserve and the primary bank regulators. This is the way the functional regulators should and will work in the environment of diversified financial institutions.

Conclusion

Controlling compliance risk may be easier said than done. Certainly, establishment of an effective enterprise-wide compliance-risk management function and program is not done overnight. Nor is it done without costs--both monetary costs and the intangible costs inherent in real cultural change. However, it is clear that all organizations must find ways to effectively manage compliance risk--and there is growing consensus within the industry that for some of the largest and most complex organizations, an enterprise-wide approach to controlling compliance risk is no longer just a "nice thing to have." Rather, it has become an essential element of effective risk management.