Mark W Olson: Enterprise-wide compliance-risk management

Remarks by Mr Mark W Olson, Member of the Board of Governors of the US Federal Reserve System, At the Fiduciary and Investment Risk Management Association's Twentieth Anniversary Training Conference, Washington, DC, 10 April 2006.

* * *

Thank you for giving me the opportunity to speak to you about one of the broad issues that you will be discussing during the next several days--the nature of risk and risk management. Today, I will offer my perspectives about risk management in general and then focus on enterprise-wide compliance-risk management, an area of risk management that has been receiving a good deal of attention lately. Risk, to state the obvious, is inherent in all activities in your industry. With the benefit of hindsight, the financial services regulators and the industry have been trying to distill the lessons learned from recent internal control breakdowns in the financial services sector. My remarks today will delve into some of the implications those breakdowns have for compliance-risk management.

Over the past two decades, we have seen remarkable changes in the global financial system. Among these changes are (1) the financial sector's increasing reliance on risk-transfer strategies and (2) the dizzying array of new products being offered to customers. Investment options continue to proliferate, as new investment products are developed and alternative investments such as hedge funds, which now total $1 trillion by some estimates, continue to grow.

Risk management in general

One of the biggest risks facing businesses and governments today is the risk of not preparing for how the world will change over the next five years. Note that I said "preparing" for change and not "predicting" change. Predicting change in a specific way is highly speculative, but planning for the inevitability of change is prudent management. A key question to ask is whether your organizations have the tools and risk-management processes that will allow them to cope with inevitable changes. As fiduciary and investment risk managers, you pay considerable attention to measuring and monitoring the risks your institutions face, and to managing and controlling those risks. You probably also devote considerable time and resources to keeping abreast of the latest advances in finance and risk management. And if you are like most risk managers, you are finding it increasingly difficult to keep up with your colleagues and competitors, because our world--especially those aspects of our lives influenced by science and technology--is changing at an exponential rate. In this regard, one of the biggest risks faced by risk managers is not being sufficiently prepared for the future. As Yogi Berra once said, "The future ain't what it used to be." Yet risk managers face the challenge of ensuring their organizations are sufficiently prepared for whatever events the future holds.

It's true that we cannot predict the future in a specific way. But if the past is any guide, we can comfortably expect that new technologies will enable us to overcome problems and challenges that today appear to be insurmountable. At the same time, however, innovation will bring new problems and challenges. As risk managers, the key question for us to answer is "How can we best cope with the dramatic changes and challenges that will inevitably occur?" Preparation is the easy answer, but foresight and discipline are also needed. At a fundamental level, managers need to make sure that their organizations have in place the risk-management policies, processes, and technologies to properly measure, monitor, and control their risk exposures. Beyond the basics, the next imperative is to do some hard thinking about the future. More specifically, managers need to conduct scenario analysis and scenario planning--and this is one area of risk management that is sometimes overlooked or not taken seriously. Scenario analysis and scenario planning are difficult; they cannot be done on the fly.

For many financial organizations, scenario analysis starts and ends with quantitative exercises that measure exposures to specific risk factors, such as changes in interest rates or credit spreads. To realize the full benefits of scenario analysis, however, the analysis must move beyond quantitative exercises. A comprehensive scenario analysis should encompass a thoughtful and thorough analysis of potential, but plausible, major changes in the economic, political, and social landscape. What are these changes? How will they affect your business? How will you respond to them if they occur? This analysis is the primary responsibility of risk management.

But scenario analysis is not the end goal. Something must be done with the results of the analysis. Management must ask itself whether the organization needs to restructure its balance sheet or modify its current risk-management strategy in order to be prepared for scenarios that may unfold in the near future. This strategizing is at the core of effective scenario planning. Some key scenarios you should consider as part of your scenario planning include how forces such as continued globalization, technological advances, and competition from product innovation will affect your particular line of business. For example, globalization makes group management and risk aggregation more challenging, and the increasing power of information technology creates both new opportunities and new risks. Furthermore, new products and new distribution channels are likely to affect your business and risk profile.

The fiduciary and investment world has not been immune to problems caused by ineffective controls. Well-publicized accounts of late trading and market timing at mutual fund firms, and the related investigations, have touched many businesses including banking, securities, and insurance firms. These types of compliance failures result in sanctions or financial loss and adversely affect the reputation and franchise value of a firm. As a result, we are seeing an increasing focus on enterprise-wide compliance-risk management systems.

The business lines and activities of financial services firms can cross 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 some of the mutual fund cases, the Federal Reserve, as the consolidated supervisor of the relevant banking organization, worked closely with the primary bank regulator and the Securities and Exchange Commission (SEC) to investigate control breakdowns. The agencies exchanged information in order to compare their findings. Findings from SEC examinations of the broker-dealers, investment advisers, and mutual fund distributors were analyzed together with findings from targeted joint reviews of the bank holding companies and the banks conducted by the Federal Reserve and the primary bank regulators. The banking agency reviews were focused on corporate-wide compliance practices and bank lending practices.

My observation is that the significant deficiencies in mutual fund practices resulted from a combination of factors and a breakdown in controls. First, mutual fund activities were not being effectively overseen by their mutual fund boards. Second, there were strong financial incentives at certain firms to increase the profitability of mutual fund activities, but the legal and reputational risks of these incentives were not appropriately addressed. Third, a lack of adequate employee training resulted in employees deviating from standard procedures, in order to accommodate certain large customers. For example, in some cases, employees granted key customers a routine waiver of redemption fees, which allowed them to engage in market timing at the expense of other fund shareholders. A stronger corporate compliance program would have enabled a local compliance officer to identify these problems and bring them to the attention of higher-level managers within the corporation.

Based on our experience in investigating control breaches in these mutual fund cases, I would like to highlight a few lessons learned. One of the most obvious to me is the need to critically evaluate unusual client relationships that require variances from standard procedures. There is an additional red flag if a high percentage of compensation is derived from a single client. Additionally, organizations should have a formal process for reviewing and approving unique products, customers, and services at the inception of the client relationship. And, finally, it is always a good idea to shine some light on areas historically labeled "low risk" to validate that assessment. The low occurrence of loss from an activity should not be the only factor considered when assessing risk.

Compliance-risk management frameworks

As these lessons suggest, compliance risk can arise when the organization fails to comply with laws, regulations, or standards of conduct. Fortunately, various models are available to help organizations manage compliance risk more effectively. A number of banking institutions have installed, or are in the process of enhancing, comprehensive, corporate-level compliance-risk management functions. Many organizations are also bolstering their compliance-risk management programs by upgrading their compliance management information systems, which allows for more-integrated and transparent analysis and monitoring. An enterprise-wide approach to compliance-risk management has proven valuable in areas such as Bank Secrecy Act (BSA) and anti-money-laundering (AML) compliance, information security, privacy, transactions with affiliates, and conflicts of interest.

A common trend for both large and small organizations is the transition away from *task-oriented* compliance programs to *process-oriented* compliance programs. Process-oriented programs require compliance to be tested and validated on an ongoing basis. In addition, fragmented and duplicative compliance activities are being scrapped for those that enable an understanding of compliance across the organization. This is not to say, however, that local compliance activities in business units are obsolete but rather they should be part of an integrated, global program. This promotes consistency in expectations, documentation, assessments, and reporting.

An effective enterprise-wide compliance-risk management program is flexible to respond to change, and it is tailored to an organization's corporate strategies, business activities, and external environment. In addition, an effective enterprise-wide compliance-risk management program requires strong board and senior management oversight.

The board of directors and senior management have different but complementary roles in ensuring the success of an organization's enterprise-wide compliance-risk management program. The board of directors is responsible for establishing a strong compliance culture that makes compliance an integral part of day-to-day operations; the board then entrusts this responsibility to managers and staff at all levels of the organization. A strong compliance culture encourages employees to raise concerns about compliance risks and the need for additional or improved controls.

Conclusion

Our review of industry best practices and an analysis of the experience of other industries suggests that organizations need to supplement their enterprise-wide compliance-risk management systems with strategic and dynamic thinking. To prepare for what may be ahead, organizations should draw not only on past experience but also employ quantitative and qualitative scenario analysis and planning. To quote former Chairman Greenspan, "The advent of sophisticated risk models has not made people with gray hair, or none, wholly obsolete."