Remarks on Enterprise Risk Management
Cathy E. Minehan

To
The New England Chapter
of the
National Association of Corporate Directors

April 6, 2004

Good Evening. I'd like to thank Joe Caruso and Pat Flynn for inviting me to speak with you tonight. The National Association of Corporate Directors plays an important role in educating directors and senior executives about the critical issues surrounding effective corporate governance. The current business climate has certainly highlighted the need to stay abreast of industry best practice and evolving statutory requirements in this area. Tonight I'd like to build upon the discussion of corporate governance and talk with you more broadly about the important role that an organization's culture plays in managing risk in the context of a broad approach to enterprise risk management.

The case for building a culture that supports enhanced risk management is compelling. By now we're all too familiar with the tales of corporate misconduct that seem to continue to make their way into the headlines. Parmalat, the Italian conglomerate, is only the latest in an unfortunately growing list of companies that have failed to operate in a manner consistent with what would seem to be fundamental business ethics. We can recount the large scale accounting irregularities at companies here in the United States that once seemed above reproach

like Enron, Tyco and Worldcom and the market timing and other irregularities that have had a big impact locally on the mutual fund industry.

Events like these in many cases have had dire consequences for the individuals and companies involved, but beyond that they have raised questions about the integrity of corporate America. While the vast majority of organizations operate in an ethical fashion, there is a real concern that these high profile instances of unethical behavior and poor corporate governance have the potential to weaken investor confidence and compromise the strength and stability of our capital markets. Consequently it's not surprising that Congress has responded with new legislation to beef up corporate governance and controls.

As I'm sure most of you know, the Sarbanes-Oxley Act of 2002 was signed into law last July. Like you, I have had to become very familiar with the requirements of this law. Both my own organization and the financial institutions that the Federal Reserve regulates have been revisiting control procedures and the role of their Boards' audit committees. The governance practices and related penalties outlined in Sarbanes-Oxley will in all likelihood serve as a deterrent to future corporate misconduct as intended. However, compliance with this

legislation alone cannot assure us that future missteps will be avoided, nor can it guarantee that companies will be successful in achieving their objectives and managing their risks. As important as the transparency and integrity of our organizations' financial reporting is, directors and senior management need to have a broader focus.

In today's environment it's easy to focus on the negative aspects of risk. We all know, however, that risk is a part of doing business and presents a variety of opportunities. Banking organizations are a good example. Financial intermediaries make their living taking on the risks faced by their customers in financing businesses and household activity. In the process they create risks for themselves as they manage the impact of markets and credit conditions on both sides of their balance sheets. And if they didn't take risks, financial intermediaries would have no purpose. Taking risks is their business; controlling that risk is a necessity. But this risk-return tradeoff is not unique to the financial services industry. Innovation would come to a halt if businesses were unwilling to accept risk. As with financial intermediaries, the key is understanding and managing the full range of potential risks facing these organizations.

I would argue that while risk management has taken on aspects of a highly quantitative science, at least for financial firms, it really does begin with a simple concept. An organization's success in managing its risks--whether it expresses them quantitatively or qualitatively--stems from its own corporate culture. If that culture is out of step with the risks being taken, or if the "tone at the top" reflects the variability of the stock market rather than a long run sense of business ethics, then most other attempts at managing risks, no matter how sophisticated, will fail. In the end, the culture created by the directors and senior officers of a corporation is the single most effective tool of risk management I can think of.

How is this culture created? Clearly every corporation will have its own particular formula, but there are a few constants. A good corporate culture will balance the firm's risk preferences with its strategic goals, incentive and compensation philosophy and corporate ethics. It will ensure that a consistent message of integrity and compliance with the law is delivered both formally and informally. And beyond this, directors and officers will ensure that the amount and type of risk that is acceptable within an organization also is reflected in its

culture. This helps everyone in the organization understand how to balance short-term profitability and long-term goals.

Now you may well be thinking all of this is so easy to say but in many instances is so difficult to do. In the late '90s, when the fates of corporations rose and fell with each uptick of the market, officers and directors believed that it was their job to ensure the company was managed so as to benefit from the rising tide. Performance was measured, incentives designed, and limits pushed to achieve what I am sure was seen as a desirable end--the welfare of the company and the related welfare of its officers and directors. It was easy to believe that the star CEO would not stay unless he or she was compensated like other stars, and if directors did not see that for themselves, consultants pointed it out. If the newest accounting techniques were not used to create the appearance of higher or more stable income flow then management might believe they had not done the best for their company and themselves as well. In fact, it is interesting to note that at least one of the difficulties in prosecuting some of the more egregious cases of corporate greed, has been the seeming lack of criminal intent. Everyone was doing it--whatever it was--and that made it not only right

but seemingly required. Thus, the question becomes, is it really possible to keep your head when all around people are losing theirs?

Of course it is, it has to be. As it is with every bubble, there are those wise participants who manage to avoid the mania. But it is not an easy task. To accomplish it leaders have to have a firm sense of what makes sense in their industries and what does not. They have to be willing to question the star CEO and each other. They have to be willing to appreciate and pay the auditor as much as the risk-taker, and they have to welcome and embrace bad news, and the people who bring it, as they would bearers of good news. There are many organizations that survived and prospered during the late '90s, through the recession and now in the recovery. They have kept their values in tact, and now, I suspect, are benefiting from the increased focus on corporate governance and their own good reputation. The right tone at the top is not easy to achieve, but if it is achieved, it is an asset that assists the whole company in sailing the often rough seas of today's competitive markets.

Now let's assume that a good corporate culture exists in an organization. What else needs to be done to ensure the organization is managing its risks? Or, perhaps, most pointedly, what process provides

officers and directors with the comfort that they will not be blindsided by some aspect of their businesses that never was on their radar screen? Setting the right culture sends an important top-down message; information from the bottom-up is necessary feedback for a good control environment. Increasingly, one way of getting that feedback is encompassed in a concept known as enterprise risk management. Unfortunately it seems to have become part of the management lexicon in the form of an acronym--ERM.

As is the case with most evolving concepts, there's no single agreed upon definition or framework for ERM. However, at the most fundamental level, ERM involves a process of risk aggregation across the activities of a firm, so that it can be assessed by top management. In the world of financial entities, risk management for many has involved looking at separate kinds of risk: credit risk, market risk, and most recently, operational risk, which results from inadequate or failed internal processes, people, and systems or from external events. Operational risk is particularly interesting in that it includes a diverse set of risks ranging from legal risks to disruptions in the weather, as well as the types of risks that result from operations themselves. To some degree, then, risk management has been approached in "silos" -

though clearly bringing together these silos is important, particularly when thinking about the critical area of capital adequacy. This approach has had the benefit of allowing risk managers and top management to start with individual areas and explore in some detail how to quantify the risks in the silo and how these risks vary over time and with changing conditions.

However, as these approaches to risk management within areas become more ingrained, it also becomes obvious that not all risks, nor sometimes not even the most important risks, are neatly covered by the three categories. Indeed, reputational risk, while very hard to quantify, has a significant bearing on the fortunes of companies financial and otherwise. Moreover, the way all risks interact with each other across organizations is important as well. This leads to the broad concept of enterprise risk management.

As I noted before, risk management has become a highly quantitative practice in most financial firms, employing as it does a number of statistical and model-based approaches to risk measurement. The same is true for ERM, though I would argue that for senior management to regard this as a "black box" process that creates a few numbers is missing the point. ERM has to be driven by top

management, its culture and its understanding and identification of risks. There are benefits to the process to be sure, but they are there only if the process is well understood by top management and is a vital part of its governance process. I would even argue that ERM done qualitatively, that is, with risks identified as significant and growing, or the opposite, is better than a quantitative approach, if the quantitative aspects are not well understood. Clearly the tools provided by ERM, whether they are quantitative or qualitative, are only useful if they can effect change in the way risk is valued.

Is ERM something you should be interested in even if your corporation is not a financial institution? I would argue that it is--that it is a natural complement to the tone at the top you have tried so hard to set. How is this? Well, most approaches to ERM require that the longer term strategic consequences of the risks and opportunities corporations face be linked to some form of risk management. ERM would have an organization systematically identify and assess risks throughout their activities, factoring in external environmental factors and company specific issues. It should inform senior management about the organization's risk profile, and the likelihood of achieving longer term goals. It should provide insights into whether the incentive

and compensation philosophy correctly rewards staff. ERM implementation can look daunting, particularly as it is usually framed quantitatively. But the concept is straight-forward, and, as I argued earlier, better a qualitative approach to start with than a quantitative one that is not well understood.

Given everything that's happening, it's fortunate that individuals like yourselves are willing to take on the significant responsibilities that have been placed on directors and senior managers. The requirements of Sarbannes-Oxley can seem overwhelming; as can the need to understanding increasingly advanced risk management techniques. The roles of directors and senior managers have never been more demanding or more critical given the perpetual state of change in which we seem to find ourselves. The examples that we've seen in the headlines have shown how dangerous it can be if we fail to set the appropriate tone at the top or ignore potential risks. By learning from the mistakes of others and gaining experience with the new legislation and evolving risk management techniques, however, the point will be reached eventually where once again directors and senior managers can be more comfortable in their positions.

In the meantime, much attention needs to focus on creating a culture that embraces good business ethics and integrity. Furthermore, an infrastructure needs to be in place to effectively identify, measure and manage the risks across the organization.

This sounds daunting, but it is doable. By using common sense, asking the right questions and ensuring that management has a broad perspective of risk, the potential for serious corporate missteps at least has a chance of being minimized.

What are the right questions? Let me suggest a few that directors and management should be asking as they think about corporate culture and comprehensively managing the full range of risks they face.

- **Does the corporation's culture currently support an appropriate level of risk taking? That is, does the "tone at the top" send the right message about limits, recognizing that each firm will have its own sense of what limits are appropriate.**
- **Have we aligned our risk profile with our strategic decision making process? Our strategies for the future can translate into more or less risk taking and we need to recognize that.**

- **Do we have a risk management program in place to help us identify and understand our most significant risks on an aggregate basis?**
- **Do we know how our risks are interrelated? Do they offset or magnify each other?**

And finally,

- **Do our directors as a group have the necessary skills to understand the business dynamics and related risks of our organization?**

Our responses to these questions can help us determine whether our organizations would benefit from a more structured ERM framework. They also will help directors understand the framework now in place.

I'd like to conclude by saying again how impressed I am by your group's efforts to enhance corporate governance nationally and in regional forums such as this. Thank you again for your invitation to speak on the critically important and integrally related topics of corporate culture and risk management. As I hope my remarks have made clear, corporate culture is the foundation for all risk management efforts and while risk management on an enterprise-wide basis offers

substantial benefits, the challenges are real as well. However, with a bit of common sense, and a willingness to work through these risk issues gradually, I believe a satisfactory approach to enterprise risk management is within our grasp.

Thank you.