From PLI's Course Handbook
Corporate Governance 2010-A Master Class
#22647

18

ENTERPRISE RISK MANAGEMENT AND GLOBAL COMPLIANCE IN THE CORPORATE GOVERNANCE CONTEXT: THE GENERAL COUNSEL'S ROLE AND THE BOARD OF DIRECTORS' EXPECTATIONS

William L. Deckelman, Jr.
CSC

INTRODUCTION

At no time in history have the challenges facing general counsels of global, publicly-held companies appeared so daunting. The global reach and interconnectedness of business combined with instant and global information access means businesses today operate, evolve and are impacted by change 24 x 7 and faster than ever before. Add to this the effects of the global economic crisis and the ardent U.S. political and regulatory response to that crisis and public company directors, general counsels and other executives will tell you it is the "perfect storm."

Enterprise Risk, Global Compliance and Corporate Governance will continue to be the general counsel's highest priorities in 2010. Enterprise Risk and Global Compliance are substantively challenging initiatives under the best of circumstances, but they become particularly difficult in times when companies are struggling to survive very tough economic conditions and resources are severely constrained. Companies expanding globally are continually faced with the challenge of identifying, understanding and applying new laws and regulations in the countries in which they operate. Of course, U.S. government regulators have adopted a more aggressive enforcement attitude and are more focused on cooperation with their global counterparts requiring extraordinary diligence in compliance areas such as the Foreign Corrupt Practices Act. Companies contracting with the U.S. government are adjusting to a raft of changes in False Claims Act compliance and acquisition regulations and new laws and regulations involving mandatory disclosure of non-compliance and organizational conflicts of interest.

Corporate Governance is rapidly changing at the same time and general counsels are required to devote an increasing amount of their time to these issues. Much of the blame for the financial crisis has been directed at "poor corporate governance" and as a consequence U.S. public companies are required to adapt to sweeping statutory and regulatory changes which materially impact governance issues, such as director elections, and require new and extensive disclosure in executive compensation, director qualifications, board governance matters such as separation of Chairman and CEO positions, and risk oversight by directors. The legislative and regulatory pendulum has swung dramatically and, in fact, it likely has not reached its apex. We now regularly hear corporate governance experts openly questioning whether the best public board directors may decide they have had enough. We are not likely to see the situation become that dire. Boards and management are resilient. They will adjust and comply. However, these changes do come with substantial costs which have real impact on the global competitiveness of U.S. companies. And boards and management are not sanguine about how far afield the SEC's new proxy access rules could take us from well settled notions of shareholder and board rights and responsibilities.

The purpose of this article is to offer perspectives from one general counsel's experiences over the past two years in leading enterprise-wide initiatives to design, organize and implement risk management and compliance programs on a global basis and in assisting the board of directors to understand and implement best practices for oversight of these management responsibilities.

THE BOARD'S PERSPECTIVE ON ENTERPRISE RISK MANAGEMENT AND COMPLIANCE

It is well understood by now that a board of directors has oversight responsibility for a public company's risk management and compliance functions. The question is how thoroughly and responsibly is the board exercising that oversight?

Certainly following the adoption of the Federal Sentencing Guidelines in 1991 boards began to take compliance more seriously. However, it was not unusual for companies to outgrow or become complacent about their compliance efforts and to resort to an ad hoc and reactionary approach to compliance. In recent years boards have become increasingly interested in knowing and validating that management has in fact implemented a systematic compliance program that in reality is effective. This increased awareness and concern is partially in response to consequential events and trends in this decade such as the Enron/WorldCom/Tyco scandals, compliance requirements under Sarbanes-Oxley, and increased government enforcement of the Foreign Corrupt Practices Act. In addition, with accelerating globalization boards have become more sensitive to the myriad laws and regulations encountered by global businesses. Boards are highly sensitive as well to vulnerabilities from technology developments, such as cyber security breaches, data loss, and risks of moving to "cloud computing." And the compliance challenges presented by the multi-jurisdictional and complex web of data privacy laws and regulations have become all too well known to directors.

Likewise, the enterprise risk management idea and discipline has been around for years and is fairly mature. However, for many companies it was not such a compelling idea that it was fully embraced by the business. In fact, enterprise risk management done right is very challenging because it touches virtually every aspect of the enterprise and is heavily reliant on information technology tools and disciplined management processes. It requires resources, investment and commitment by the business. As with compliance functions, many companies experimented with bits and pieces of enterprise risk management and approached "risk" in an informal and ad hoc manner. But the global financial events of 2008 dramatically sharpened the focus of boards on the actual effectiveness of the risk management functions on which companies were relying to identify and manage serious risks to the

business. Recently adopted SEC disclosure rules will also now require more attention from directors in terms of how they exercise their risk oversight responsibilities.

In both areas, Enterprise Risk Management and Global Compliance, boards now are insisting on *visibility*. Directors want to see for themselves and thoroughly understand how these functions are designed and they want to have enough information to enable the board to judge for itself that management has adequately addressed risk and compliance. *A general counsel should ensure that the directors are afforded this opportunity in a meaningful way.*

A FRAMEWORK FOR ENTERPRISE RISK MANAGEMENT

The first step then for management is to design the framework for an Enterprise Risk Management ("ERM") program. ERM is a broad "umbrella" concept – it addresses several kinds of risk, including Compliance. A novice in these disciplines can easily access enough information through the internet, educational materials and books, professional associations, and from dozens of IT and software providers and accounting and consulting firms that he or she would quickly become overwhelmed and find it difficult to know where to start. Indeed, if a company has the luxury, retention of a consultant to assist in the design of the framework can be very valuable. *In any case, focus on sifting through the data as efficiently as possible to gain a solid understanding of the fundamentals – then move forward with ideas for a framework that fits your company's business, culture and particular circumstances.* It is important to begin the process of vetting ideas for the framework with other corporate and business units. *It is critical that you come out of the gate with a framework and implementation plan that is pragmatic, fully supported by executive management and the business, and is clearly designed to result in real business value through improved business processes.*

So what should the general counsel's role be at this stage? Certainly the general counsel will be leading the design of the compliance program. However, in its basic form ERM comprises not only compliance risk but also strategic, operational and reporting risk. *While the general counsel will not be "expert" in the non-compliance risk areas, the general counsel could well be in the best position among executive management to lead collaborative discussions of the ERM framework design. The general counsel by experience should have a solid intuitive feel for these risks and how they interrelate and the general counsel should have the best understanding of the framework which will optimize the board's visibility into the company's ERM program and the board's ability to fulfill its oversight role.*

Before I describe CSC's ERM framework, it is important to touch on board and CEO sponsorship of an ERM initiative. I am very fortunate in that the CSC board of directors and CEO enthusiastically support, and in fact, were the impetus for our company's ERM program. This is absolutely critical. *If you are a general counsel interested in initiating steps toward a formal ERM program and you do not have the full support of your board of directors or CEO, then you must expend your first efforts establishing that support.* An ERM initiative without this level of support will simply not succeed.

We set about designing the CSC ERM framework to be as straightforward and pragmatic as possible. *A fundamental tenet of our program was that it would be designed to ensure that responsibility and "ownership" of enterprise-wide risk was shared among the entire executive team.* This was not to be viewed as some isolated and "out of touch" corporate function. Our CEO insisted on this. As a result, we formed an ERM Committee comprised of our CEO and executive officers reporting directly to him. This is an ERM Committee of twelve executive officers. The executive officers on this committee represent the most senior leaders of our business sectors and other executive officers such as our CFO, our VP of Human Resources, our VP of Strategy, Mergers & Acquisitions, and the General Counsel. Our CEO is the Chairman of the ERM Committee and the General Counsel and our Chief Compliance Officer are designated as responsible for providing administrative assistance to the Committee.

The ERM Committee's charter describes the committee's responsibilities as management of the company's "GRC" functions – Governance, Risk and Compliance.

As an approach to management of risk, we adopted the four categories of risk outlined in the COSO (Commission of Sponsoring Organizations of the Treadway Commission) framework – strategic, operational, reporting and compliance risk. We have assigned individual members of the ERM Committee as responsible leaders for these areas. Our Vice President of Strategy, Mergers & Acquisitions is responsible for strategic risks. The General Counsel is responsible for compliance risks, the CFO for reporting risks, and our operations executive committee for operations risk. *Accountability is an important feature of the ERM framework – it ensures steady progress toward achievement of the goals of the program.*

We have developed a standard methodology for risk assessment in each of these four categories. Strategic risk was the first category assessed. The assessments involved corporate strategic risks and strategic risks for each business sector. Executive management identified and rated the severity of these strategic risks and developed contingency plans to address each of the risks. This activity was included as an integral part of our overall annual corporate strategic planning process which culminated in a two-day meeting

of executive management with the CSC Board of Directors to review strategic plans.

The General Counsel and our Chief Compliance Officer are heavily involved in the risk management activities for the operational and reporting risk areas as well. Each group is required to establish a regular process and annual cycle for its risk assessments and mitigation plans. The end result for each group is a prioritization of risks, mitigation plans for each risk, and determination of the investments and funding required for execution of mitigation plans. The latter stage of the annual process is designed to coincide with the company's annual budgeting activities. All of the activities and reports of these groups are reported to and discussed with the ERM Committee on a regular basis. In turn, the General Counsel reports on these activities to the Board's Audit Committee at each quarterly meeting and periodically (at least annually) to the full Board of Directors.

This approach is only one of many available. We have found it to be a very workable framework for CSC. *Again, a key to success of an ERM program is that it be straightforward and practical and that the corporate and business sector executives see the program as delivering bottom line value to their business as a result of better clarity of risks and improved business processes.*

Importantly, for the Board of Directors this framework and approach assures the directors that management is disciplined and systematic in how it addresses risks across the enterprise. The formal process affords the Board the visibility it needs to exercise the proper level of diligence in its oversight of risk.

A FRAMEWORK FOR GLOBAL COMPLIANCE

As described above, CSC's compliance activities are treated as one of four key areas of enterprise risk for purposes of our ERM program. Of the four areas, however, it is the broadest and most active.

Historically, CSC's compliance program had developed primarily in the company's government contracting business sector. In fact, due to the extensive and rigorous compliance requirements of federal contracting, the company had a mature public sector compliance program. As the company ventured into the commercial sector in the 1990's the compliance efforts were primarily led by the Legal Department and key compliance requirements were addressed, but largely on an ad hoc basis. As the company grew globally it became increasingly difficult to effectively manage the program and to assess whether there were compliance gaps that were not being filled.

In 2008 we concluded that a coordinated and formal program framework was needed which would allow executive management to better understand and effectively manage CSC's compliance risks and allow the Board to improve its oversight of compliance and periodically evaluate the overall effectiveness of the compliance program. The approach and the details of the framework were first reviewed with the Audit Committee and subsequently with the full Board of Directors who fully endorsed the approach.

A key part of the recommended approach was the hiring of a dedicated Chief Compliance Officer. As we initiated the program CSC appointed a full-time Chief Compliance Officer who reports to the General Counsel. At first blush this could appear as though we had established a strong "centralized" or "corporate" compliance function. Actually, we designed the compliance framework so that while it has ultimate governance and reporting in through the corporate legal function to the Board of Directors, the intent is to keep the corporate staff small and instead to carry out the majority of compliance functions in the business units themselves. *This design was purposeful for a very key reason – we want to ensure that the CSC businesses understand that they "own" compliance as much as "corporate" owns compliance.* A compliance mindset and culture can only be created if the people involved in the day-to-day business of the company learn to think this way and apply this approach in the way they routinely do business. Therefore, our Chief Compliance Officer must be highly collaborative and capable of persuading operations management to become actively engaged in the compliance processes.

In designing the compliance program we and the Board specifically took into consideration the Federal Sentencing Guidelines requiring that the "governing authority" (i.e., the Board) be knowledgeable about the content and operation of the company's compliance plan and that it exercise reasonable oversight with respect to the implementation and effectiveness of the plan. As discussed below, we have designed much of the process and reporting functions of our compliance plan to ensure we and the Board meet these requirements.

In addition, the Federal Sentencing Guidelines require that operational responsibilities for the program be delegated to specific individuals who shall be given adequate resources, appropriate authority and direct access to the Board. *Accordingly, our Chief Compliance Officer has "dotted-line" reporting directly to the Audit Committee and it is clearly understood that the Chief Compliance Officer may at any time engage in direct discussions with the Audit Committee Chairman or the Committee.*

As with ERM, we have approached compliance from the point of view that compliance is important not only because it is "required," but also because it adds bottom line business value as a result of clearly understood and more

efficient business processes (not to mention, of course, the value of avoidance of many types of "damages" such as regulatory fines and damage to reputation).

To address the specific substantive compliance areas applicable to CSC we have categorized our global compliance obligations into 13 subject matter areas, as follows: International Trade; Global Anti-Corruption; Global Data Privacy and Data Protection; Public Sector Contracting; Government Affairs; Global Intellectual Property; Global Environmental, Health & Safety; Global Labor, Employment & Immigration; NYSE and Corporate Governance; SOX and other SEC compliance; Global Tax; Global Antitrust; and Global Records and Information Management. We have ensured that we have subject matter experts who are responsible for each area and they, in turn, form working groups to ensure that they have identified key compliance issues on a global and enterprise-wide basis for the company.

We have established a Global Compliance Council which includes representatives from all key corporate support organizations and from all material business units. We ensured that the council membership was diverse and included a good cross-section of individuals from around the world and who would be serving in support or operational roles where they could be influential in establishing the compliance functions we have planned. This council will serve as our communications path, both incoming and outgoing, with the rest of the CSC organization as we move forward with the compliance program.

We have initiated many actions to launch the compliance program, including a maturity and capability assessment to assist us in benchmarking our program by evaluating exactly where our strengths and weaknesses lie. The program is designed to operate on an "annual cycle" basis so that the culmination of activities every year coincides with our budgeting process leading into the next fiscal year. Each year the Global Compliance Council will develop the *Annual Compliance Plan* and that plan will address the following matters. First, it will include an *Overview of the compliance program*, describing the organizational and governance structures and the reasons for those structures as well as the overall compliance processes related to development and implementation of the current Annual Compliance Plan. Second, it will include an *Annual Risk Assessment and Mitigation Plan* which will include a report of the results from the annual risk assessment activities and a prioritization and mitigation plan for each area of compliance risk. Third, *Annual Action Plans* will be included. These are specific plans for each corporate and business unit indicating risks that will be addressed in the coming fiscal year, how they will be addressed and related resource and budget requirements. Next, there will be an *Annual Communication and Training Plan* which addresses communication and training priorities for the fiscal year and the related resource and budget requirements. Next, an *Annual Monitoring and Audit Plan* will be included

which addresses how key risks will be monitored during the fiscal year and a specific compliance audit plan for CSC's Internal Audit organization. Finally, there will be *Annual Effectiveness Evaluation* which represents the Global Compliance Council's and executive management's evaluation of the effectiveness of the overall compliance program. It is this section of the Annual Compliance Plan that the Audit Committee and the Board will refer to as it conducts its evaluation of the effectiveness of the compliance program.

In summary, the Annual Compliance Plan in effect documents the most important activities occurring during the year under the compliance program. During the course of the year, the General Counsel, and periodically the Chief Compliance Officer, gives regular reports of activities to the Board's Audit Committee and annually to the full Board of Directors.

These activities require a substantial amount of work. But again the intention is to ensure that this is not simply "busy work" but rather that it is valuable work that ensures we are identifying tangible areas for improvement and in the end that CSC does in fact have an effective compliance program. Our Board of Directors requires this kind of program and now is in a position to have a more detailed understanding of how management views and deals with compliance risk across the enterprise.

CORPORATE GOVERNANCE, THE GENERAL COUNSEL AND THE BOARD

Corporate governance in general has, of course, been evolving rapidly for most of this decade and general counsels in recent years have been spending an increasing percentage of their time advising their boards on these changes. As mentioned in the Introduction, many more changes are just being implemented or are on the horizon and will certainly have a great impact on how general counsels and boards are spending their time in the coming year. In particular with respect to risk oversight, the SEC's new proxy disclosures rules which will go into effect shortly will require specific risk-related disclosure in two respects.

First, the rules require disclosure about the board's role in risk oversight, including how the board performs its risk oversight responsibilities. If the general counsel and the board have implemented an ERM framework as discussed above, much of the work will have been done here and it will be a matter of preparing the proper disclosure. However, as it will be the first time the company has disclosed the way the board actually functions as it performs this important role, the general counsel and the directors should be collaborating on the disclosure and the message the board wants to send to the public in terms of its risk oversight. This discussion will probably highlight the importance of the respective risk oversight roles of each of the board committees and the full board. For example, each of the Audit Committee, the Compensation Committee and the Nominating and

Corporate Governance Committee view risk from different perspectives given the scope of their responsibilities. While the Audit Committee often will take a leading role in risk oversight, it will be important for general counsels to spend more time with the Compensation Committee (see below) and the Nominating and Corporate Governance Committee to ensure that these committees have defined their approach to risk oversight. The general counsel then will need to synthesize and integrate these activities into a framework for the full board to review, discuss and approve.

The second risk-related aspect of the new proxy disclosure rules requires disclosure of situations where a company's compensation programs could result in material risks to the company. General counsels by now have been spending a great deal of time with their compensation committees developing and implementing a methodology to survey and analyze their various compensation programs across the company and evaluating potential risks against the stated standard of "reasonably likely to have a material adverse effect on the company." Again, this will be new disclosure for companies so general counsels should expect a substantial amount of review and collaboration with their compensation committees as the disclosure is developed.

So what will the board of directors expect and need from general counsels in light of the recent surge in legislative and regulatory changes in corporate governance? Obviously, the boards want to be informed of the changes. However, they need the information presented in an understandable and actionable way. They expect general counsels to advise them on the real impact of the changes, how other companies are responding to the changes, and what alternatives are available to the directors in terms of response and actions. Most certainly this means increased preparation time as general counsels and their staffs absorb, understand, and interpret the new laws and regulations and, in turn, survey best practices and prepare to advise their boards on actions they should consider. It also means there will be a great deal more governance dialogue between the general counsel and the directors outside of the boardroom which should afford the opportunity for the general counsel to forge even stronger relationships with the directors.