COMMITTEE ON INSURANCE COVERAGE LITIGATION

Coverage

Section of Litigation
American Bar Association

Timothy W. Burns and Linda B. Foster, Committee Co-Chairs
Editor in Chief: John C. Tollefson

Published by LexisNexis
Volume 14, Number 6, November/December 2004

Articles

Emerging Corporate Governance Standards for Risk Management and the Lawyer's Role

by Mark Siwik and Randall Davis

I. Introduction

Perhaps for the first time in its fifty-year history, risk management has become a topic of corporate governance. Since 1999, corporate directors and senior management of publicly listed companies in the United Kingdom have been required to identify and manage material risks.[1] Similarly, the passage of The Sarbanes-Oxley Act of 2002 is forcing senior management of American companies to identify and review financial risks and then report what measures are being taken to mitigate those risks.[2]

(Continued on page 14)

Mark Siwik is Senior Counsel with Risk International, where he focuses on the handling of complex insurance claims and working with senior management to improve the corporate risk management function. Mark can be reached at msiwik@riskinternational.com.

Randall Davis, MBA, joined Risk International in 2002 where he handles many of the strategic, analytical and technical aspects of risk management including quantitative modeling, statistical analytics, qualitative and quantitative research, competitive and organizational dynamics, and strategic risk management advisory services. Randall can be reached at rdavis@riskinternational.com.

Emerging Corporate Governance Standards

(continued from page 1)

Complying with these emerging standards of corporate governance for risk management is easier said than done. To begin with, there is confusion as to what constitutes best practices for risk management. In the words of one respected industry group, "no common technology exists, and there are few if any widely accepted principles that can be used by business leaders as a guide in developing an effective corporate risk management function."[3] The lack of a widely accepted framework for risk management in turn creates questions about how well companies manage risk. For example, a survey of senior management published by Financial Executives in November 2001 showed that 65% of executives lack confidence that their existing risk management function identifies and manages all potentially significant business risks.

If senior management lacks confidence in their risk management processes, is it any wonder that corporate boards are uninformed? A recent McKinsey survey involving 200 directors representing over 500 boards, determined that almost 40% of the directors did not understand the risks faced by their companies.[4] One could speculate about how many directors had similar doubts but did not like to say so.

Who should the board and senior management look to internally for advice on best practices for risk management? The obvious choice is the risk manager but in many companies this is only a partial solution because senior management and "board members have yet to be convinced of the relevance of the traditional risk manager."[5] Too often, the risk manager is perceived as a mid-level functionary tasked with buying insurance and settling claims. Instead, companies are likely to turn to a senior executive, such as the chief financial officer or the general counsel. Determining which senior executive is the right person to lead the charge of creating, appraising, or overseeing the risk management function must be done on a case-by-case basis. Much depends on the personal interest and leadership skills of the person in question and the company's culture.

Because the company lawyer (whether in-house or outside counsel) always participates in some aspect of the risk management function, we decided to write this two-part article. The goal of the first section is to provide an overview of the evolution of risk management so that any company lawyer (or for that matter any senior executive) can lead or participate in an intra-company discussion about improving the corporate risk management function. For those lawyers who want to contribute more to the risk management function, the second section provides specific advice on how to go about it.

II. <u>What is Corporate Risk Management?</u>

This section describes how the corporate risk management function has evolved since its inception in the 1950s.[6] Our purpose is to provide a sufficient grounding for the company lawyer to participate in discussions about corporate governance standards for risk management with the board of directors and/or other senior executives such as the chief executive officer and the chief financial officer.

Risk can be simply defined as deviation from the expected and it exists in all areas of business. In fact, risk and return is what business is all about. Risk also has a positive and negative aspect, which in turn leads to the definition of corporate risk management—taking deliberate action in accordance with the company's strategic objectives and board policy to increase the odds of good outcomes and reduce the odds of bad outcomes.

As you read through this section, try not to see risk as simply controlling or preventing the downside. Dan Borge, former partner and managing director at Bankers Trust and author of the highly popular risk management book, *The Book of Risk*, wrote in his opening paragraph:

> The term "risk management" is loaded with connotations of caution and timidity, carrying unpleasant reminders of dreary sessions with insurance agents and infuriating lectures from parents on the dangers of having a good time. People who think about risk management at all are likely to think of it as a grim necessity, at best.[7]

Moreover, it is important to recognize that risk management is pervasive—it touches everybody and pervades all aspects of personal and corporate life. Mr. Borge continues:

> The point is not to *become* a risk manager but to become a *better* risk manager, since we are all risk managers already. We make risk decisions every day, often without thinking about it. . . . I am not suggesting that you agonize over every little choice you make, but I am suggesting that you can and should think more carefully about those decisions that could have important consequences for you.[8]

Because we live in a world of uncertainty, we are all risk managers already. Therefore, any gains in our understanding of the risk-reward relationship and how to live with uncertainty can profoundly affect the success of both our organizations and our personal lives.

A. The Risk Management = Insurance Era

Despite its broad and pervasive nature, corporate risk management has been viewed historically as a narrow function primarily concerned with insurance. This historical view arises from the fact that insurance—the transfer of a small loss (the premium) to a third party which accepts responsibility for a possible large loss—has been an industry since the bartering of risk began in London coffeehouses (today Lloyds) in the late 1600s. By the 1940s, insurance had matured to the point that companies could buy it for a number of hazards ranging from potential loss of property to worker's compensation. By the 1950s, corporate America and business academia recognized that the mere handling of insurance for a variety of risks had become so complicated and time-consuming that it was deserving of a full-time position known in most companies as the "insurance manager."

Writing for the Harvard Business Review in 1956, Russell Gallagher, the insurance manager of Philco Corporation in Philadelphia, suggested that the position of insurance manager be renamed "risk manager." Gallagher argued that the risk manager should be an executive and that corporate risk management should concern itself with four basic questions:

- How should a company go about analyzing its risks? What factors should it look for? What difficulties is it likely to encounter?
- What efforts should be made to avert or abate risks? What kinds of steps are possible? What are the pitfalls and dangers?
- When should a company insure itself against risks? How should commercial insurance be purchased? How can insurance costs be kept to a minimum?
- What problems arise in the administration of risk management? What kind of authority should the risk manager have, and how can he get cooperation in carrying out his program?[9]

Almost 50 years later, Gallagher's questions remain relevant. The problem is that the passage of time has not led to the adoption of a simple and comprehensive risk management framework that answers these questions.

> ***"A focus on corporate insurance led to conventional thinking that risk management means insurance — thinking that, unfortunately, is still prevalent today."***

A major reason for the lack of a widely accepted framework is that insurance industry marketing efforts drove the development of the risk management position as opposed to critical thinking on the subject. In 1966, ten years after the Gallagher article, the Insurance Institute of America developed insurance-related courses leading to the first certification of risk managers. Newly certified risk managers often then would join the American Society of Insurance Management, which today is known as Risk & Insurance Management Society (RIMS). This focus on corporate insurance, unfortunately, led to conventional thinking that risk management means insurance—thinking that, unfortunately, is still prevalent today.

By the mid-1970s, leading thinkers began recognizing that risk management was much more than insurance and that its practice was becoming disjointed and fragmented. In 1976, *Fortune* magazine published a special article entitled "The Risk Management Revolution" by Felix Kloman, a risk management expert and visionary. Kloman recognized that companies had begun slicing corporate risk management into pieces without conscious thought or deliberation. Financial officers created risk management tools (hedging, interest swaps etc.) to deal with the myriad of financial risks (currency levels, interest rates etc.) confronting businesses. Operations focused on product quality, product safety, and business continuity. Executives and boards concerned themselves with growth and optimization of capital.

Even the insurance function became fragmented and disjointed. The conservation of physical assets and the control of insurance purchasing became the province of the treasurer or the chief financial officer. Meanwhile, the law department toiled away at controlling losses and submitting insurance claims, sometimes in disagreement with the risk manager who fretted about trying to explain the rising costs of premiums to senior executives uninterested in anything other than numbers. In fact, some companies were nearly torn apart on the issue of coverage for environmental and asbestos losses, with risk managers and lawyers often at odds over the meaning of policy language.

The insurance wars over asbestos and environmental contamination did lead to one positive revelation:

> The truth, as risk managers know, is that as soon as the insurance industry is faced with major risks — latent diseases, product liability, AIDS, among others — it runs for cover and leaves industry to its own devices. Basically, society cannot expect much help from insurers in sorting out its risk problems because insurers are interested not in risk reduction. . .but in risk predictability.[10]

The visionary, Felix Kloman, put it this way: insurance ". . . is an industry trying to build its edifice on the sands of certainty and predictability in a world in which uncertainty and unpredictability are the bedrocks."[11]

B. Struggling Toward A Holistic Approach

In his seminal 1976 article, Kloman called for a holistic approach to risk management that would begin with a "clear, written statement of policy supported by the board of directors, designating the administrative authority for coordinating the risk management effort."[12] In 1990, Kloman described this holistic approach as follows:

> [R]isk management should be seen more as a function than a specific person. It should be practiced by many levels of management, with coordination and guidance from a senior level. . . . How will the new risk management process function? Ted Ferry of the University of South Carolina suggests:
>
> > We need an overview of checks and balances that studies every interface and assures that all risk elements are considered. We need persons who can see the big picture, overview, coordinate, assimilate and bring every aspect of risk into focus.
>
> Using the new definition and these comments, risk management becomes a planning and strategic function, not solely an assessment, financial or safety one.
>
> The new risk management will be an outgrowth of earlier efforts and disciplines. It will be a true synthesis of many of the earlier ideas that have approached risk from a more limited vantage point. The synthesis will be composed of ideas and efforts from the following areas:
>
> - Insurance management and risk funding.
> - General management theory and practice, from Henri Fayol to Peter Drucker.
> - Macro-risk assessment and decision risk theory and practice, addressing such areas as nuclear, natural disaster, and environmental risk.
> - Quality assurance methodology, for both products and services.
> - Loss prevention, safety, and security engineering.
> - Crisis management.
> - Financial risk maneuvers, including currency hedging and interest rate swaps.
> - Risk psychology, education, and communication.
> - Statistics and actuarial sciences.
>
> The new risk manager will not have to be, and certainly cannot be, an expert in each of these areas. He or she will, however, have to be a manager in the broadest sense of the word, one who is at least conversant with the applicable disciplines and willing to look broadly and holistically at risk as it affects the organization.[13]

Kloman's clear and succinct description notwithstanding, the last 25 years has witnessed a sea of confusion and paper about the best way to create a comprehensive risk management framework that is simple enough to allow for a common way to identify, manage, and report risk with oversight from senior management and the board.

"The last 25 years has witnessed a sea of confusion and paper about the best way to create a comprehensive framework that is simple enough to allow for a common way to identify, manage, and report risk with oversight from senior management and the board."

The most common nomenclature given to this effort to create a holistic approach is "enterprise risk management." Several factors have prevented enterprise-wide risk management from achieving a best practices standard. First, "enterprise," in our view, is the wrong word because it suggests that the solution to risk management is a cookie-cutter checklist or comprehensive template that will completely satisfy reporting obligations and corporate governance standards. The better word is "strategic" because each organization is unique, with its own risk culture, appetite, processes, and personalities and as such each organization must adapt and apply "enterprise-wide" thinking to its strategic objectives.

Second, enterprise risk management has failed because organizations are made up of people who are products of their training and experience. Consequently, they make little effort to understand the methodology, benefit, or even to recognize integrated risk concepts. Kloman put it this way: "Financial risk managers are . . . too focused on currency levels and interest rates. . . . Safety people don't [even] admit that financial risk management exists."[14] The rationalization offered for this compartmentalized thinking is that if the individual components, or "silos," of total risk are optimized, then the whole must therefore be optimized.

Third, and perhaps most importantly, far too much time and attention has been spent trying to perfect a model of enterprise risk management that captures and classifies every form of risk confronting an organization. Our view of the typical risk categories is shown in Figure 1. We favor this simple approach because it uses the category "Other Risk" to avoid getting caught up in the minutia of risk categorization. There has been no agreement on what constitutes total risk to an organization, and we're not sure that there ever will be. Moreover, it's not as necessary to have widespread agreement throughout the business world on how best to classify risk as it is to appreciate that corporate governance standards are moving toward using strategic risk management to address the uncertainty inherent in managing a business.

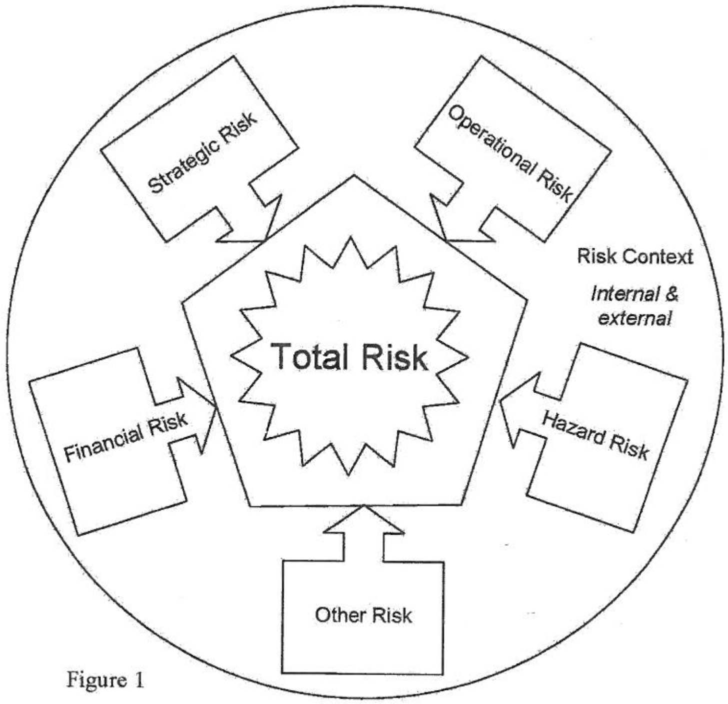

Figure 1

We believe that it is just a matter of time until the emerging corporate governance standards requiring boards and senior management to become more involved with risk management settle on a strategic risk management framework that equates with "best practices." How quickly this best practices standard develops will depend on four factors:

- How quickly will companies recognize that risk management requires a senior person or several senior people to champion and lead the effort?
- How quickly will companies recognize that the proper function of the internal champion is to ensure that all facets of the organization are following board level policy on risk management, using techniques that are consistent with such policy and appropriate for the particular context at issue?
- Will companies be able to avoid falling into a trap of jargon and an overly complicated risk management model that is unrealistic or impractical to implement?
- How successful are companies in acknowledging existing risk management expertise while motivating the people with such expertise to buy into a common risk management communication and reporting framework that is simple and easy to use?

In the next subsection, we review the two leading models of strategic risk management.

C. Leading Risk Management Models

The most talked about model at the moment is COSO's Enterprise Risk Management Framework.[15] This model is designed to help a company meet its strategic, operational, and reporting and compliance objectives by focusing on the interrelationships of risks across business units and at every level of the company. The desired result is consistent risk and control consciousness throughout the organization. The model also represents the first effort by a large segment of the U.S. business community, the auditors and financial controllers, to create a comprehensive framework (previous models have been largely the suggestion of an individual or two).

At present, the COSO model is in the draft stage, with its final release scheduled for mid-2004. Nevertheless, in its present form, we do not believe it is where senior management and corporate boards should start in reviewing their risk management function. First, perhaps due to the kind of people COSO represents (auditors and controllers), the model focuses too much on control and the negative aspects of risk. Another top strategic risk management thinker, Mark Carey, comments:

It has been our experience that one of the biggest challenges for ERM across all organizations, is to get the various risk management related functions, teams and initiatives to work effectively together, across organizational silos. We constantly see the conflicts and turf wars between different risk functions. The team assembled for this effort appears to be heavily weighted towards individuals with experience in areas related to audit and controllership. Involving a more diverse risk management team in the development and oversight of this document would have likely developed a framework that more fully addresses the spectrum of risk management processes, activities and philosophies necessary to create an effective ERM program.[16]

A second limitation to the COSO framework is that it violates the KISS rule (Keep it simple, stupid). Boards and top risk executives will not champion a methodology that only increases the complexity of their oversight mandate. While the COSO framework does cover many of the main points of a good risk management program, the reader can quickly become lost in the over-complex and jargon-laden wordiness.

In our view, the risk management model worthy of becoming the corporate governance standard is Standards Australia's AS/NZS 4360:1999[17] model for risk management. Like the COSO framework, it sets out to establish a "generic framework for establishing the context, identifying, evaluating, treating, monitoring and communicating risk."[18] But unlike the COSO model, it is a "model of clarity," "exceptionally well written," and "the gold-standard for all others, worldwide."[19] The framework is a simple 23 pages, and approaches risk management with a recognition that simplicity will contribute to adoption of the standard.

Like essentially all risk management frameworks, it describes the iterative process of risk assessment and risk response in multiple steps:

1. Gain active and ongoing support of senior management.
2. Develop the organizational risk management policy.
3. Communicate the policy.
4. Manage risks at the organizational level.
5. Manage risks at the program, project, and team level.
6. Monitor and review.

Further, the model relies on a simple convention for managing risk throughout the organization, which is depicted in Figure 2 below:

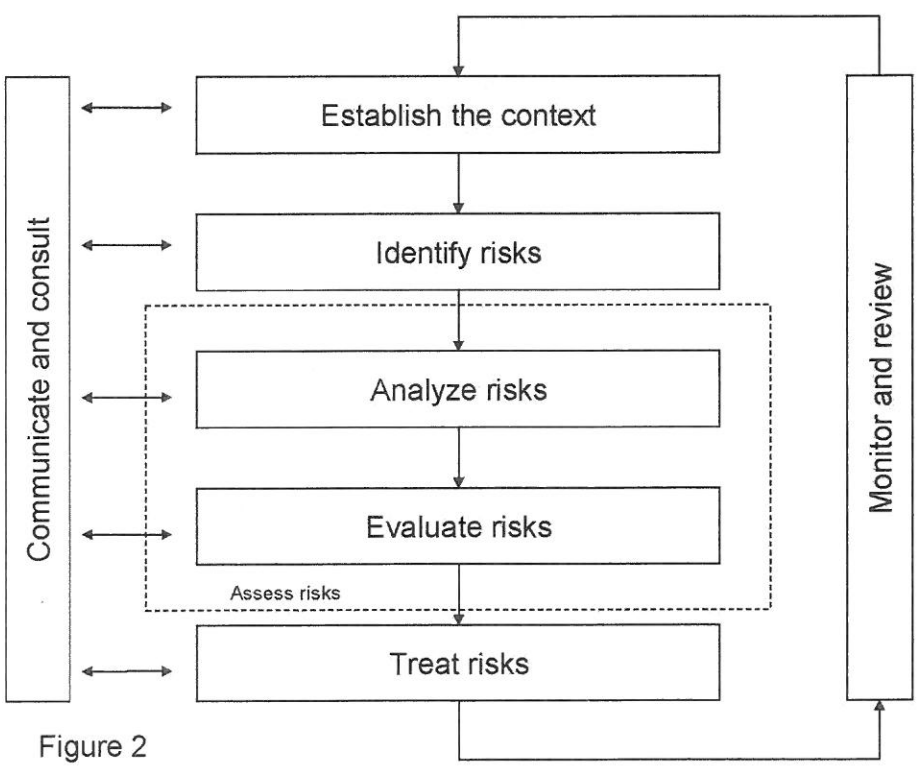

Figure 2

What makes this approach unique in our minds is that it does not try to come up with a universal risk management technique that applies to everyone and everything. The goal instead is to ensure there is a base commonality for (i) approaching decisions in a manner that increases the odds of a good outcome and reduces the odds of a bad outcome and (ii) reporting risk management practices in such a manner that appropriate oversight can be exercised by senior management and the board.

III. Impacting the Corporate Risk Management Function

> ***"Risk management, practiced correctly, is the responsibility of more than one person or department, it is a multidisciplinary function drawing from expertise and leadership throughout the organization."***

This section is intended to provide information to help the lawyer contribute effectively to the risk management function. At the outset, however, it is important to note that the lawyer is by no means the only member of senior management qualified to lead and manage the risk management function. In fact, if there is one trap to avoid, it's pre-determined thinking that risk management is best administered by one section of the company, whether it be legal, financial, operations, or audit. The best solution will vary from company to company and it will depend on the interest level of the people involved and the culture of the organization. More importantly, risk management, practiced correctly, is the responsibility of more than one person or department; it is a multidisciplinary function drawing from expertise and leadership throughout the organization.

The first subsection below explains how to approach the leadership issue in terms of evaluating present risk management processes and implementing a new framework consistent with emerging corporate governance standards. The second and third subsections give two practical examples of how a lawyer can work with other members of the organization to improve the risk management function.

A. Leadership

Effective leadership requires starting with the end goal in mind. Following the model proposed by Standards Australia, the role of the board and senior management is to develop the organization's risk management policy and to monitor the organization's risk portfolio for compliance with that policy. Items that may be included in the organization's risk management policy are:

- the objectives of the policy and rationale for managing material risks;
- relationship between the policy and the organization's strategic plan;
- extent or range of risks to which the policy applies;
- guidance on what may be regarded as material risk;
- who is responsible for managing material risk;
- support/expertise available to assist those responsible for managing risk;
- the level of documentation required; and
- the plan for reviewing organizational performance in regard to the policy.[20]

Once the policy is in place, it is a matter of communicating the policy and ensuring that risk is managed at the organizational level through the strategic planning process and within each sub-organizational area (e.g., operations) or specific project. The two vehicles most commonly used to ensure that a risk management policy is established and that risks are appropriately managed and reported are (i) a multidisciplinary risk management committee and (ii) a chief risk officer ("CRO"). Again, there is no right answer in terms of whether to create a risk management committee or a CRO or both. The critical thing is to recognize the importance of senior leadership.

A pioneer in the use of risk management committees and CROs is James Lam, who is credited with becoming the first-ever CRO, "inventing the job title in 1993 when he was working for U.S. financial services giant GE Capital."[21] Drawing from the example of the chief information officer, Lam made the CRO responsible for "integrating all forms of risk within the firm—including credit risk, market risk and operational risk—and elevating the awareness and understanding of these risks to the board level."[22] The resulting benefit is twofold: (i) it designates someone sufficiently senior to make certain that corporate governance standards are met and (ii) it ensures that there is at least "one person [who] can answer the board's questions about what are the greatest risks facing the company and how we are dealing with those."[23]

> ***"In picking someone to oversee risk management, worry less about about specific risk management credentials and more about who will command the respect of the board and senior management while working effectively with line managers to ensure compliance with board policy."***

Chairpersons of risk management committees and indeed, CROs, have come from all walks of life within organizations: "[A]ccording to surveys, they are auditors, actuaries, financial engineers, strategic planners, lawyers, investor relation specialists, line operation managers, [insurance] risk managers, even HR specialists."[24] In our view, we would worry less about specific risk management credentials and more about who will command the respect of the board and senior management while working effectively with line managers to ensure compliance with board policy. Such a person should possess strong analytical ability and proven skills to lead, manage and communicate:

> The CRO need not be the smartest person in the company, nor the person with the most degrees, nor the loudest, nor the most energetic, anymore than the CEO has to be all these things. Rather, a CRO's success derives from an ability to see the big picture, grasp complex topics, identify and analyze the key issues, and lead the entire process.[25]

Clearly, the training lawyers receive makes them as qualified as anyone to oversee the risk management function.

B. Working as a Team to Manage Total Cost of Hazard Risk

A good and fairly simple first step to take toward improving the risk management function is to increase the coordination between insurance purchasing, typically a treasury function, and the law department. In our experience, the financial managers generally fret about the cost of insurance and the legal managers worry about the expense of managing claims but too often they don't work together.

The typical advice given to lawyers desiring to influence the risk management process is to "take a more active role in negotiating policies."[26] While having a lawyer review the policy forms is helpful, the real question on most minds outside the legal and financial departments of an organization is whether the organization is getting true value not only from its insurance but the efforts made in general to manage hazard risks. Let's suppose that an insurance broker has just presented his annual renewal summary to a company, which contains another hefty premium increase. How do the financial and legal managers respond to the tough questions from other members of senior management and the board? How do they evaluate the broker's statement that the renewal package is the best deal available?

The metric designed to measure the cost-effectiveness of hazard risk management (e.g., first party, third party claims) is a tool known as Total Cost of Risk (TCOR). Because the cost-effectiveness of hazard risk management is measured for all types of industry and size of companies in an annual Total Cost of Risk survey, each company can benchmark itself against industry peers and over several years for trending purposes.

Computing Total Cost of Risk is straightforward:

premiums
+
self-insured losses and legal fees
+
broker fees
+
administrative costs
= TCOR

The first step is to add up all premiums, including any premium tax. Don't include life or health benefits, as these are not within the scope of this metric, but do include worker's compensation. Most companies will have auto, property, general liability, excess general liability (or umbrella), and worker's compensation policies. Others will have coverage for crime, directors and officers, employment practices, errors and omissions, cargo, aviation, fiduciary, environmental, etc., depending on the size, complexity and activities of the business.

Next, total all the losses paid or amounts expected to be paid (loss reserves) that were not covered by insurance. Include any outside defense costs or legal fees that were not covered by insurance associated with these claims. Next, add the fees paid to the broker for his or her service. Finally, add administrative costs, which are the costs to manage the insurance program. In large companies it is usually the costs of the risk management department. In smaller companies it may be a portion of the controller's salary and benefits if he or she spends a portion of his or her time on insurance matters. In either case don't forget the cost of benefits and expenses when calculating employment costs. Some companies outsource some aspect of hazard risk management to a third party, and in those cases, simply put the third party's annual fees into this category.

To make TCOR really useful, it must be known how it compares with the experience of competitors. To do this, TCOR needs to be expressed as a percent of revenue, or as a dollar cost per $1,000 of revenue (take the TCOR for a given year and divide it by revenue for the same year). For most companies, this will provide a result between 0.5% to 2.5% of revenue (sometimes expressed as $5.00 to $25.00 per $1000 of revenue). Then compare the results to the reported survey results. Every summer, the Total Cost of Risk survey is produced in conjunction with RIMS, the Risk and Insurance Management Society.[27]

Getting the legal and financial departments to work together to benchmark the organization in terms of controlling insurable costs is just the first step. A second step would be to assemble a multidisciplinary team to assess how well the company is managing the insurable risk in the first instance so that the team can meaningfully discuss the degree to which the organization should transfer risk, the cost-effectiveness of insurance vs. self-insurance, and the type and amount of insurance that should be purchased. In the end, this kind of discussion, as opposed to just gathering data from operations to submit to underwriters and allocating premium costs to the various business units, is true risk management.

C. A Team Approach to Worker's Compensation

Worker's compensation is another troublesome area where a lawyer interested in risk management can make a difference. Historically, worker's compensation was designed as a covenant between employers and employees. Employees give up their right to sue their employers for work-related injuries and diseases in exchange for quick and economical wage-loss replacement, sensible and required medical care, and, when an absolute medical cure is not possible, a disability payment to compensate for permanently-lost future earning ability. Without this covenant, "the entire U.S. economy would be mired in endless litigation, expense, and impaired productivity."[28]

Notwithstanding its noble objectives, many organizations and states are experiencing precisely what the worker's compensation covenant was created to prevent. California, for example, is reporting permanent partial disability claims at 181% of the national average.[29] Further, the number of major permanent disability claims in California has more than doubled from 1995-2000.[30] Government solutions to the problem have not stemmed the tide: "Estimates of the legislative 'savings' have simply not found their way into the worker's compensation claims-file results."[31]

So, what is going on here? In our view, the frequency and severity of worker's compensation claims are tied to other organizational and external risk factors that are not being managed by those tasked with handling worker's compensation. In many organizations, one or two people try to do it all—keep track of workplace injuries, tally the costs of claims, place the insurance coverage, and try to get injured workers back to work. Moreover, when workers are truly injured, they are "dumped" into the lap of the worker's compensation manager and they are no longer a concern of their former manager or department. They become second-class citizens of the organization with insufficient effort made to bring them back to full productivity.

To truly manage a worker's compensation program, a broad risk management approach is required. This approach will track the obvious costs as well as the often hidden costs of lost productivity/ efficiency, overtime, continued benefits, claims administration, insurance premiums, spoilage, diminished customer service, OSHA penalties, damage to tools and equipment, decreased employee morale, record keeping, lost sales, and diminished reputation. All of these hidden costs are typically outside the control of the worker's compensation manager. Further, senior management must see and respond to the interrelationship of risks. One common example is the spike in worker's compensation claims when a plant closure or workforce reduction is announced.

In the end, a successful worker's compensation program depends on the ability of an organization to manage risk in a comprehensive manner. This will require a policy that has the support of senior management, operations, financial and legal, each of which fulfills their defined roles and responsibilities. The policy must be communicated and then managed within the specific operations in accordance with the company-wide policy. A successful worker's compensation program will also use simple measurement and monitoring tools to ensure proper review and reporting.

IV. Conclusion

Emerging standards of corporate governance are requiring more involvement by the board of directors and senior management in the corporate risk management function. For many companies, the initial challenge is to simply understand the present state of their corporate risk management function and determine how to improve it using the tools and frameworks in existence today. We hope this article will help lawyers contribute to the process, particularly because so many organizations look to the lawyer for advice on what constitutes compliance with corporate governance standards.

We also hope that this article will help lawyers determine how best to participate in the risk management function. In fact, depending on the lawyer's level of interest and the culture of the organization, it may be appropriate for the lawyer to oversee the function. Regardless of the depth or breadth of the lawyer's involvement, there are two areas, hazard risk and worker's compensation, that are good places to start in helping any organization achieve a best practices standard for risk management.

1 *See* Institute of Chartered Accountants, *Internal Control: Guidance for Directors on the Combined Code* (The Turnbull Report) (1999).

2 *See* Sarbanes-Oxley Act, Pub. L. No. 107-204, §§ 302, 906 (2002).

3 *Enterprise Risk Management Framework (Exposure Draft for Public Comment)*, Committee of Sponsoring Organizations of the Treadway Commission, at 1 (2003).

4 *Living Dangerously: A Survey of Risk*, The Economist (Jan. 24, 2004).

5 *The Boardroom's Burden,* Risk & Insurance at 18 (November 2003).

6 In writing this section, the authors wish to acknowledge the work of Felix Kloman, who has done as much as anyone to record the history of risk management and chart its future.

7 Dan Borge, *The Book of Risk*, at 3, (John Wiley & Sons, Inc.) (2001).

8 Dan Borge, *The Book of Risk,* at 4 (John Wiley & Sons, Inc.) (2001).

9 R. Gallagher, *Risk Management: New Phase of Cost Control* at 76, Harvard Business Review (July 1956).

10 Christ Best, *London Perspective*, Risk Management (Feb. 1989).

11 Felix Kloman, *Risk Management Agonistes*, Risk Analysis, Vol. 10, No. 2 (1990).

12 Felix Kloman, *The Risk Management Revolution*, Fortune (July 1976).

13 Felix Kloman, *Risk Management Agonistes*, Risk Analysis, Vol. 10, No. 2 (1990).

14 Felix Kloman, *Risk Management Agonistes*, Risk Analysis, Vol. 10, No. 2 (1990).

15 COSO is a voluntary private sector organization comprised of the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, The Institute of Internal Auditors, and the Institute of Management Accountants. COSO is dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

16 Mark Carey, *COSO Enterprise Risk Management Framework Comments*, at 2, (DelCreo Inc. 2003).

17 For more information and a copy of the draft, see Standards Australia at www.standards.com.au.

18 Joint Technical Committee-OB/7, *AS/NZS 4360:1999 Risk Management*, at iii, (Standards Association of Australia) (1995, 1999).

19 Felix Kloman, *Congestion vs. Clarity,* Risk Management Reports at 1, Vol. 30, No. 10 (2003)

20 Joint Technical Committee-OB/7, *AS/NZS 4360:1999 Risk Management*, at Appendix B, (Standards Association of Australia) (1995, 1999).

21 M. Hanley, *Another C Change*, CFO Europe (Mar. 20, 2002).

22 M. Hanley, *Another C Change,* CFO Europe (Mar. 20, 2002).

23 M. Hoffman, *Chief Risk Officer Role Still Being Defined*, Business Insurance (Feb. 23, 2004).

24 J. Miccolis & C. Lee, *Implementing Enterprise Risk Management: The Emerging Role of the Chief Risk Officer*, Tillinghast Towers Perrin (Jan. 2002).

25 *Are You CRO Material?* Risk Management at 24 (Sept. 2000).

26 M. Milford, *Insurance Worries: Post-9/11, General Counsel Adopt Role of Corporate Risk Managers*, National Law Journal at A-27 (Sept. 30, 2002).

27 The 2003 report can be ordered at rims.advisen.com/RIMSSurvey.

28 Stanton F. Long, Briefing note *To: Employers That Pay Worker's Compensation Costs in California,* at 1, (Marsh) (2003)

29 Stanton F. Long, Briefing note *To: Employers That Pay Worker's Compensation Costs in California,* at 2, (Marsh) (2003).

30 Stanton F. Long, Briefing note *To: Employers That Pay Worker's Compensation Costs in California,* at 2, (Marsh) (2003).

31 Stanton F. Long, Briefing note *To: Employers That Pay Worker's Compensation Costs in California,* at 2, (Marsh) (2003).