



# ***Risk Management Reports***

Volume 30, Number 5      May 2003

□ Copyright 2003, by H. Felix Kloman and Seawrack Press, Inc.

## **Enterprise Risk Management: Past, Present and Future**

*This is a paper that I first presented to a meeting of the Institute of Internal Auditors, in September 2002. I later used it in revised versions in Stockholm in November 2002 to the NORD RM Conference and in New York in March 2003 to the Annual Conference of the National Association of Commercial Contract Managers. My readers will recognize many of the ideas, as most of them appeared in these pages over the past few years. It is a summary of my current thinking.*

**Introduction** Publications, conferences, organizations and vendors constantly trumpet the phrase “enterprise risk management” as if it is the Second Coming or the next great thing since the Internet. Is it a passing fad or can it address some of the pervasive ills that have infected our organizations over the past decade? Do we need the adjective “enterprise” or any of its sister phrases, such as “integrated,” “business,” “holistic,” or “strategic” (which I confess to using)? Isn’t all this simply “risk management?” I believe our discipline is important but we must bring it back into perspective. One way to do that is to retrace its historical roots before considering its current posture and where it is likely to lead us. My first step is a short walk through history. Then I describe where we are now, and, finally, I offer some thoughts for the future, as we address three critical management issues.

For me, two authors frame our discussion, pointing out a remarkable paradox.

Anthony Storr, in his 1966 study of saints, sinners, madmen and gurus, *Feet of Clay*, wrote that doubt and uncertainty “are distressing conditions from which men and women passionately desire release . . . . As a species, we are intolerant of chaos and have a strong

predilection for finding and inventing order . . . . Certainty is hugely seductive.” The human condition does not like uncertainty.

We should like it, however. The Nobel laureate physicist Richard Feynman countered that “it is in the admission of ignorance and the admission of uncertainty that there is hope for the continuous motion of human beings in some direction that doesn’t get confined, permanently blocked, as it has so many times before in various periods in the history of man.” Progress is dependent on taking risk.

Uncertainty is a human paradox: we fear it but need it! In the past century most corporate, nonprofit and governmental analyses of and responses to both uncertainty and risk were conducted on a fragmented basis. We focused primarily on specific fears and harmful events, looking only at the negative sides of risk to the exclusion of possible benefits. We responded too often to those who had something to sell, financially or politically.

In the future we will look at risks affecting the whole of an organization and its place in the community. We will address both upside and downside consequences and our view will be enterprise-wide, integrated and holistic. The result will be a more intelligent balance between potential benefits and harms. We will increase the confidence of stakeholders in our organizations and make them more resilient in a day and age of increased uncertainty. This is the real goal of risk management.

**Where Have We Come From?** Human history is a record of attempts to understand unexpected events. Floods, storms, lightning bolts on the one hand, and success in battle and love on the other were all attributed to either the gods or Fate. To avoid misfortune and gain success, men and women prayed to and propitiated gods, singular or plural, including the sacrifice of human beings. Overwhelming uncertainty was the primary fact of life. Later, as we began to keep oral or written histories, we found that some events occur within a pattern. Using this knowledge we built reserves to tide us over when misfortune struck. Farmers allowed their lands to lie fallow once every seven years and took advantage of spring floods. As commerce developed throughout the Mediterranean Sea, shippers wisely split their goods among several vessels to reduce the chance of total loss from weather, pirates or Sirens. Men learned to challenge uncertainty and to determine the causes, other than heavenly wrath, of various misfortunes. They began to create measurable risk from immeasurable uncertainty. This, as Feynman points out, is the essence of humanity: the quest for the new even as we try and explain the old.

Peter Bernstein’s *Against the Gods: The Remarkable Story of Risk* is the best chronicle of our centuries-old progress from reliance on the gods to the transformation of some uncertainty into “risk,” through the application of experience, numbers and probability.

He writes: “The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than a whim of the gods and that men and women are not passive before nature. Until human beings discovered a way across that boundary, the future was a mirror of the past or a murky domain of oracles and soothsayers who held a monopoly over knowledge of anticipated events.”

Bernstein describes the efforts of well-known trailbreakers such as Pascal, Fermat, Edward Lloyd, Bernoulli, Bayes, and Bentham. He also introduces us to many less-known names such as Pisano (Arabic numerals), Cardano (probabilities of dice), John Graunt (statistical tables), Abraham de Moivre (the “bell” curve and standard deviation), and Francis Galton (regression to the mean).

But it was the 20th century in which we made the most progress in measuring and understanding risk. Here are some of the milestones:

- Otto von Bismarck introduced social security and workers’ compensation in Germany in the late 1800s, from which these ideas spread to Europe and the United States in the early 1900s
- Frank Knight’s *Risk, Uncertainty & Profit* (1921) celebrated the prevalence of surprise and separated risk from uncertainty. He cautioned against over-reliance on extrapolating the past into the future.
- John Maynard Keynes’ *Treatise on Probability* (1921) cited the importance of perception and introduced us to the Law of Great Numbers.
- Von Neumann and Morgenstern (1926 and 1953) created the theory of games and strategy and suggested that the goal of not losing is often superior to that of winning.
- Markowitz (1952) developed portfolio analysis, including new aspects of returns and variances.
- We formed new associations representing students and practitioners of the discipline, including the Risk & Insurance Management Society (1975), followed by counterparts in Europe, South America, Africa and Asia, the Society for Risk Analysis (1980), London’s Institute of Risk Management (1986), the Global Association of Risk Professionals (1996), and the Professional Risk Managers International Association (2002). Older organizations, such as the Institute of Internal Auditors, and the Risk Management Association (formerly Robert Morris Associates), incorporated risk management within their mandates.

- Gustav Hamilton, of Sweden's Statsforetag, created in 1974 a "risk management circle" that first described the interaction and integration of all the elements of the process.
- Daniel Kahneman and Amos Tversky published their "prospect theory" in 1979, demonstrating that human nature can be perversely irrational, especially in the face of risk, and that the fear of loss often trumps the hope of gain.
- The "Precautionary Principle," an idea that first surfaced in Sweden in 1969, was embodied in the UN World Charter for Nature in 1982.
- In 1983, Bill Ruckelshaus, Director of EPA, gave his seminal speech, "Science, Risk and Public Policy" at National Academy of Sciences, bringing risk analysis to center stage in government and public policy circles.
- Beginning in the mid-1980s, national commissions created new standards and guidelines on risk: the Treadway Commission in the US, that led to the COSO guidelines (1987), the Cadbury Commission (and following Hempel and Turnbull Commissions) in the UK (1992), the Australian/New Zealand Risk Management Standard – the first in the world (1995), followed by Canada (1997) and Japan (1997) and the UK (2001 and 2002).

**Where Are We Now?** Risk management in 2003 is recognized as an integral part of sound management. It is taught worldwide in more than 100 universities and graduate schools. Yet, because of the continuing inability or unwillingness of many of its practitioners in the separate sub-disciplines to communicate with each other, we lack a common understanding of its meaning.

The word "risk" itself is subject to several interpretations. It can mean "chance of loss," a physical property that is insured, or "a measure of the possibility of unexpected outcomes," the definition that I prefer. The safety, public policy and insurance communities continue to use risk in its limited, negative sense, while financial practitioners see it in its larger sense, encompassing both upside and downside consequences. The International Standards Organization now defines risk as "the combination of the probability of an event and its consequence," noting that "consequence may be either positive or negative." ISO adds a footnote suggesting that, "in some situations, risk is a deviation from the expected." This is a major step forward.

John Adams, in his 1995 book *Risk*, sees it as a cultural construct that “illuminates a world of plural rationalities.” Risk, to him, is a “balancing act” in which the actors “balance the expected rewards of their actions against the perceived costs of failure” in a world in which expectations and perceptions are constantly changing, in large measure as a result of our multiple responses.

However we define “risk,” “risk management” is our discipline for dealing with uncertainty. According to Peter Bernstein, “the essence of risk management lies in maximizing the areas where we have some control over the outcome, while minimizing the areas where we have absolutely no control over the outcomes and the linkage between effect and cause is hidden from us.”

Over the years the process of risk management has been encrusted with many overlapping steps, complicating what should be simple. The process has two easily remembered steps: Risk Analysis and Risk Response. Risk Analysis includes identification of possible unexpected events, their measurement in terms of likelihood, consequences, and public perceptions, and their assessment in terms of an organization’s objectives. Risk Response encompasses the controls adopted to balance risk, measuring and monitoring performance, and communication with stakeholders. The discipline answers the questions “what could happen?” and “what should we do about it?”

Current problems include the often conflicting and confusing “languages” of different practitioners, many of whom are intent on protecting their own traditional “turf,” such as derivatives, the environment, health and safety, security, contingency planning or insurance. This inevitably leads to a continued interest in tactical, rather than strategic, responses to risk (buying liability or property insurance; managing currency and interest hedges; reducing employee injuries; protecting environmental resources, etc.) But who is watching the entire store? Cross-turf problems such as the recent examples of outrageous executive compensation and perks, excessively compliant accounting, governance riddled with conflicts of interest, and the failure to communicate intelligently with stakeholders call for a more integrated approach to risk management.

New public accounting and stock exchange guidelines from such diverse areas as North America, the UK, Germany, India and Malaysia, plus new laws (Sarbanes-Oxley in the US) create altered responsibilities for governing boards. They must now assure themselves of the depth of risk analyses and the scope of responses.

This in turn stimulated a new executive position in many corporations, the Chief Risk Officer. James Lam created this new responsibility, first at GE Capital in 1993 and later at Fidelity Investments. CROs are now found today in more than 150 major corporations. In addition, in the absence of any group leading enterprise risk management, the internal auditing profession moved into this vacuum, suggesting that its members help create the function. The Institute of Internal Auditors has published

several intelligent and practical monographs on the process, conducted numerous global conferences and stimulated new training such as Control Self-Assessment (CSA). It is a natural role for internal auditors, who generally report to both the CEO and the governing board. A question remains, however. Does the practice of risk management conflict with the traditional requirement for auditor independence?

Despite these current problems, I see a growing consensus on the critical steps in risk management:

- Board and senior management commitment
- Broad view of risk encompassing *both* reward and penalty
- Common framework for the integrated analysis of all risks
- Single independent leader or coordinator for the process
- Bottom-up risk assessments, continuing periodically
- Necessity for clear and timely data
- Two-way communication with key stakeholders (this is the most often overlooked aspect of today's risk management)
- Goal: to build and maintain stakeholder confidence through improving stakeholder "value," creating a healthy internal risk culture

**Where Are We Going?** I believe that risk management will become a critical part of strategic planning. While the sub-disciplines of finance, safety, public policy, insurance, and security, etc. will be tactically linked, they will be coordinated so that an organization can reach its overall goal of creating and maintaining public confidence. Given that we can never anticipate all possible outcomes in an increasingly volatile world, contingency or business continuity planning will become a major responsibility of the senior risk officer. Finally, organizations will acknowledge that risk management is not the privileged province of specialists but the responsibility of *all* employees. Risk management will become part of the organization's culture.

The greatest area of change will be improvement in communication with stakeholder groups, including employees, customers, suppliers, lenders, investors, regulators, communities and the public at large. It is now risk management's weakest link. When we should communicate? How do we do it? How do we create a two-way dialogue?

In addition, risk management can help organizations solve three major current and future issues:

- Credibility: the events of 2001 and 2002, affecting governments, nonprofits and for-profit corporations alike, demand new steps to re-establish stakeholder confidence.
- Resilience: today our organizations are even more vulnerable to the unexpected. How should they prepare? Can they react and survive? Is it time to re-create the idea of redundancies?
- Perspective: for too many years corporations, particularly in the developed world, fostered the illusion that an emphasis on short-term results will satisfy their stakeholders. It hasn't worked. We now need to restore the long view and alter organizational culture accordingly.

Why not re-phrase René Descartes' *cogito ergo sum* - "I think, therefore I am?" to *periclitor ergo sum* - "I risk, therefore I am." Taking risk is the defining element in human existence. We should relish, not avoid it; balance, not eliminate it.

**Conclusions:** Risk management remains a developing discipline, even as it expands to encompass the entire enterprise. It embodies the basic caution that we can never know the future. We can only prepare for it more intelligently. As Steve Hagen concluded in *Buddhism – Plain and Simple* (Charles E. Tuttle, Boston 1997): "Underneath the ground of our beliefs, opinions and concepts is a boundless sea of uncertainty." Risk management is the fragile vessel on which we sail this boundless sea. Certainty is always beyond our grasp.

I've been involved with risk management since the mid-1960s, and I admit to a degree of proximity that distorts my own perspective. So I close with two haiku that suggest that my views should be treated with some degree of skepticism and caution.

First, from the poet Basho:

A cicada shell;  
It sang itself  
Utterly away

Or, as J. W. Hackett expressed it in another haiku:

Another sermon—  
Wafting through words without end,  
The smell of coffee!

Yes, freedom is that space in which contradiction can reign; it is a never-ending debate.

**Salman Rushdie, *Step Across This Line*, Random House, New York 2002**

### **Governance Standards: Australia and United States**

Governance requires control and control requires an understanding of risk. Corporate governance is now a major topic of conversation in many parts of the world. The subject is hardly new: it began with the Treadway Commission (US), the Dey Commission (Canada) and the Cadbury, Hempel and Turnbull Committees in UK, plus the mandates of the OECD, and KonTraG in Germany. With the bursting of the technology bubble and the disclosures of serious malfeasance by executives and many of their advisors, we are being forced to review general principles of sound governance and practical changes for re-establishing stakeholder confidence.

The press is awash with commentary. The US Congress passed the Sarbanes-Oxley Act and the SEC will shortly promulgate new rules. Associations and conference organizers rush to discuss the subject. I take the perspective is of the risk manager and suggest three recent publications for review.

1. Australia Draft Standards Standards Australia, along with Standards New Zealand, the initiators of the first risk management standard (AS/NZS 4360), offered in January 2003 draft suggestions for new guidelines on corporate governance. Copies are available at [www.standards.com.au](http://www.standards.com.au) or by email to [sales@standards.com.au](mailto:sales@standards.com.au). Australia created five drafts, all of which have the goal of strengthening external confidence. All focus on the “disclosure of material information” including “foreseeable risk factors.” All are notable for their brevity. The following comments refer primarily to their risk management implications.

- DR 03025: Good Governance Principles: Section 3.6 defines a different but equally important role for “other stakeholders” in an organization. This is an important distinction.
- DR 03026: Fraud & Corruption Control: This draft refers to pertinent material in AS/NZS 4360 and includes an excellent appendix summarizing the elements of a sound fraud and corruption prevention plan. The definition of “risk,” however, is too vague: “the chance of something happening that will have an impact on objectives.”

- DR 03027: Organizational Codes of Conduct: A critical ingredient is the importance of unimpeded incident reporting.
- DR 03028: Corporate Social Responsibility: This section addresses the integration of social and environmental concerns into operations, recognizing that an organization has responsibilities “over and above” purely legal ones. The draft suggests that a corporation prepare a “sustainability reporting” each year in its annual or a separate report.
- DR 03029: Whistleblowing Systems for Organizations: This is a serious problem. One recent report noted that 69% of all whistleblowers were ultimately fired from their jobs. Australia outlines a mechanism for “encouraging the reporting of corrupt practices, breakage of the law, and matters detrimental to the organization.” It also creates a plan for protecting and preserving, where possible, the anonymity of the person(s) making an allegation in good faith.” Here is an area where a risk manager should take the lead in improving what is, by all accounts, a flawed system.

2. Governance Perspectives The Institute of Internal Auditors published in February 2003 a booklet summarizing contributions made to its October 2002 Corporate Governance Summit, in New York City. Its articles are as good a synopsis of current thinking as I have read. The best is the interview with Arthur Levitt, Jr., former SEC chairman, who wrote: “I believe that directors who have the greatest stake in the company would tend to have the best possible motivation to do the best they can for the company,” and he added that the power of “embarrassment and humiliation” is a stronger deterrent than any specific penalty.” For copies contact [www.theiia.org](http://www.theiia.org).

3. Commission on Public Trust and Private Enterprise In June 2002 The Conference Board, in New York, convened a 12-member, “blue ribbon” panel to “address the causes of declining public investor trust in companies, their leaders and America’s capital markets.” The Commission’s findings and recommendations were issued in February 2003 (contact [www.conference-board.org](http://www.conference-board.org) for a copy). The report has three sections: Executive Compensation, Corporate Governance, and Audit and Accounting. Again, rather than analyze this entire 46-page booklet, I urge risk managers to read and absorb this exceptional document, and especially its dissenting opinions. Here, however, are several comments that pertain directly to the risk management discipline:

- The authors urge increased transparency (fast becoming a cliché!) and disclosure.
- “The corporation’s interests, as well as those of *other stakeholder constituencies* (my italics), are best served with a shareowner base that holds its investment for the long term.”
- The Commission cited a CNN/USA Today/Gallup poll in July 2002 that noted that small business owners (75%) and military officer (73%) are the most trusted in our society, compared to CEOs of large corporations at 23% and car dealers at 15%. This clearly states the scope of the problem!

- A board's core responsibilities include understanding the issues, forces and *risks* (my italics again) that define and drive a company's business.
- "The audit committee and any other committee of the board dealing with risk management should review and update this risk-based plan (on the company's risks and vulnerabilities) on an annual basis." Are risk managers prepared to construct, present and defend such a plan to the board annually?

I've always been impressed by the U.S. Supreme Court Justice Louis Brandeis, a very responsible man. He once commented, "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." I think that is terrific. So if I were to put forward one point in this whole area (corporate governance), it would be just that—the need for sunlight and electric light, the more of it the better.

**Sir Adrian Cadbury, interview "Let There Be Light," *Internal Auditor*, February 2003**

**Risk Management Reports**, published since 1974, is a monthly electronic publication of Seawrack Press, Inc. Copyright 2003, by Seawrack Press, Inc. All rights reserved. ISSN 0199-6827. Full copies of all prior issues to January 1994 can be found for subscribers at the Archives & Index page of the website <[www.riskreports.com](http://www.riskreports.com)> by using the name and password given to each subscriber. Issues prior to 1994 are available from the publisher.

Permission is granted for reproduction of individual articles from this publication providing that appropriate credit is given and a copy of the reproduced text is sent to Seawrack Press, Inc.

Subscription Price: Electronic transmission - US\$60 per year  
Group subscriptions at reduced rates are available.

Editor and Publisher: H. Felix Kloman  
Copy Editor: Ann B. Kloman  
Graphic Designer: Sarah P. K. Smith  
Website Manager: RiskInfo, Larkspur, California, USA  
61 Ely's Ferry Road  
Lyme, CT 06371-3408 USA  
Telephone: 860-434-2917  
Telefax: 860-434-3917  
Website: [www.riskreports.com](http://www.riskreports.com)  
Email: [fkloman@aol.com](mailto:fkloman@aol.com)

