

# A Risk of Too Many Risk Standards?

Sixteenth Annual International Symposium of the  
International Council On Systems Engineering (INCOSE)  
8 - 14 July 2006

Copyright © 2006 by Robert N. Charette  
President, ITABHI Corporation  
11609 Stonewall Jackson Drive  
Spotsylvania, Virginia 22553  
Contact: Charette@itabhi.com  
Published and used by INCOSE with permission.

The importance of risk management as an organizational discipline has grown steadily over the past 35 years, reflecting the marked shift in society's perception of the risks with which it lives. Issues that once were taken for granted (e.g., that nuclear power is safe and efficient; that our food, air, and water supplies are safe; and so on) are now seen in a new light.

Events such as Three Mile Island, Chernobyl, and Love Canal; the advent of AIDS and BSE, or mad cow disease; the institutionalism of terrorism; the Challenger and Columbia shuttle disasters; recurring power outages; the globalization of competition and outsourcing of both blue- and white-collar jobs; the rise of corporate governance; the debate over global warming and genetically modified foods; the responses of governments to natural disasters such as tsunamis, earthquakes, and hurricanes -- to name just a few -- have all contributed to a heightened public awareness of personal risk not observed until recently.

In the 1980s, German social scientist Ulrich Beck coined the phrase "the risk society" to describe this societal shift in risk awareness. This shift can be encapsulated as follows:

- The public's consciousness of the risks involved in what were once perceived as ordinary aspects of daily life has increased;
- There has been an increase in the perceived uncertainty that surrounds these risks;
- The public's reliance upon institutions and experts for managing and controlling risks has increased;
- Simultaneously, the level of public trust in these institutions and experts to manage risk effectively has decreased. (Hinchliffe 2000)

The public demand for better management of risk across all aspects of society has helped fuel the need for defined standards. Twenty-years ago when this author was writing his first book on software risk management, most software and non-software industry acquaintances didn't understand either the concept or the need for such a book. Today, these same people want to know why software-related risks aren't being regulated.

**Risk Standard Proliferation?** The multiplicity of risk standards that have been published over the past decade reflect the multiplicity of risks that concern different segments of society. These standards in turn reflect the different experiences and perceptions of what risk is and is not, as well as how it should be addressed and managed. Just as a cow looks differently to a butcher than to a microbiologist or a veterinarian, risk looks differently to a doctor, lawyer, engineer, business executive or the proverbial man in the street.

The multiple definitions of risk that the standards currently contain, for instance, merely reflect the different perspectives, experiences, custom and needs that different segments of

society have in the way of understanding and managing risk. Standards mirror society's perception of the need to do something about risk as much as they do the true need to manage a specific risk. They often reflect a response to a tragic event as well. Thus, in a situation that involves the possibility of legal actions such as torts, for example, risk will likely be defined and handled differently from one that does not. This can be seen in standards relating to the identification and management of risks in avionics, medical or nuclear power equipment.

The problem caused by the multiplicity of risk standards (as well as other types of standards) was recognized in the 1990s by the various international and national standard bodies. In the area of risk management specifically, the International Standards Organization (ISO) and Institute of Electrical and Electronic Engineers (IEEE) standard organization initiated several efforts to address this issue. One was the agreement reached in 2003 by ISO and IEEE to use IEEE Standard 1540:2001 on software risk management as a single standard for both organizations. This was accomplished in 2004, when ISO/IEEE Std 16085:2004 "Information technology; Software life cycle processes; Risk management," was published.

ISO also had started in the late 1990s an effort to harmonize risk management terminology used in its standards. As the working group tasked with this effort discovered, this was not a simple, straightforward task freed from politics, conflict or controversy. However, in 2002, ISO Guide 73:2002 "Risk management; Vocabulary; Guidelines for use in Standards," was agreed and published. Guide 73 has done a very good job at trying to provide definitions of risk and management approaches that can be used by a wide variety of industries and disciplines. Its approach has been to provide predictability of terminology while simultaneously providing for flexibility of use and adaptability in practical situations.

Once ISO Guide 73 was published, ISO and IEEE agreed that the standards addressing risk management should begin to be revised to adopt its terminology. ISO/IEEE Std. 16085:2004, for instance, began an immediate revision process to harmonize its terminology with that of ISO Guide 73's terminology. Many other ISO/IEEE standards that discuss risk and/or its management are also beginning to adopt Guide 73's terminology.

In addition, ISO requested the ISO/IEEE 16085 planned revisions not just cover software engineering but systems engineering as well. This has meant that various standard working groups involving ISO/IEEE 16085 on software and systems engineering risk management, ISO/IEEE 12207 on software development processes, ISO 15288 on systems engineering, ISO 15939 on measurement, among many others, are all working to harmonize their respective standards, including risk-related terminology.

**Proliferation or Practice Problem?** This author, through the auspices of the Cutter Consortium, has conducted two international surveys (in 2002 and again in 2006) on the state of practice of risk management in the IT community. (Charette 2002, 2006) The 2006 survey indicates that about 80% of organizations (who answered the survey) are claiming to be practicing risk management, with 66% of these organizations indicating that they are using a disciplined, repeatable and measurable process. While the percentage of organizations claiming to do risk management has remained fairly stable over the past four years, the survey suggests that the formal practice of risk management has grown by about 25% during this time.

During the course of our 2006 survey, we asked our survey takers what they perceived were the three major weaknesses of risk management. The top three weaknesses given were the difficulty in getting an accurate estimate of the level of risk encountered (46%), the difficulty of getting organizational buy-in (34%), and the difficulty in separating risks from problems (32%). When we looked deeper into the results of this question, we found that these same relative results held for organizations practicing formal risk management. However, for those organizations

indicating that they were practicing informal risk management, the same two top weaknesses also were the same. However, 33% of these organizations listed as their third major weakness the lack of a consistent definition of risk. This compares to only 23% of organizations that practice formal risk management which found this to be an issue of concern.

From both our 2002 and 2006 survey results, the problems arising from a lack of a consistent definition of risk became less important as an organization became more experienced in practicing formal risk management. One reason may be that the vast majority of people in organizations practicing formal risk management had received training in risk management. This suggests that training, along with following a formal risk management process, can help reduce the “risk definitional” problem that seems to be such a concern.

**One Universal Risk Management Standard?** I, as an IEEE and ISO risk management standards working group chair for the past seven plus years, can understand the angst that multiple risk standards can cause probably better than most people. During ISO/IEEE 16085 development and revisions, we have had to review every standard involving the management of risk and figure out how we can all “play nice together.”

However, over the next few years, I believe the on-going standard harmonization efforts should reduce the problems currently being encountered. Furthermore, I believe that as more organizations receive training in risk management and practice risk management in a disciplined manner, the perceived problems associated with “risk standard proliferation” will dissipate.

Furthermore, it should be remembered that the purpose of standards is to provide a *minimum* practice that the international community, defined through the voting procedures used by international and national standard organizations, have agreed need to exist. More formally, ISO/IEC Guide 2:2004 Standardization and related activities -- General vocabulary defines a standard as, “A *document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.*”

Standards represent the current social as well as technical beliefs of what make up an acceptable practice or standard of care. They provide a baseline or benchmark to allow objective observers to judge whether the practice as agreed exists or not. They don’t necessarily define the quality of implementation of practice, nor can they possibly provide insights or solutions for every possible situation an organization wishing to use a standard might encounter.

Generally, every five years standards are reviewed to determine whether they need to be revised or eliminated. These reviews provide opportunities to improve or refine a standard based upon experience of those applying them. No standard is ever perfect, and I suggest that those disagreeing with the risk management standards get involved in them by joining the standard bodies. ISO Guide 73 on risk terminology will be up for revision within the next two years, for example.

As a chair of a risk management standards group for the past seven plus years, and as a practitioner of enterprise, program and project risk management in government and commercial organizations around the world, I don’t think a single, universal risk management standard is necessary or even desirable. Risk, after all, reflects economic change and human inventiveness: there are undoubtedly new types of risk being created at this very moment that will require new thinking (and terminology) on how they are approached.

Furthermore, I fail to see how a “proliferation of risk management standards” would be solved by adding yet another risk management standard from an organization such as INCOSE or anyone other for that matter, as has been suggested. Before such an approach is adopted, I believe that a little more reflection is warranted on what really would be gained -- and what

unintended consequences might arise -- before such an effort is undertaken.

Finally, some are suggesting that INCOSE is very well placed to be *the* coordinator/arbitrator of risk management standards. Part of the rationale given is that INCOSE is well-connected to a myriad of defense industry and government organizations, several of whom feel that they have been left out of the conversation on risk management standards convergence. However, he warned that the world is moving quickly towards the practice of enterprise risk management (ERM), where systems and software engineering risks are but a part of the totality of risks to be identified, assessed and managed. The stakeholders in the ERM world might not view INCOSE as the organization best positioned to represent their concerns, and would likely vigorously disagree to such a notion.

### **References**

- Charette, Robert N., "The State of Risk Management 2002: Hype or Reality?" Cutter Consortium, 2002.
- Charette, Robert N., "Risk Management 2006: A Comprehensive Survey," Cutter Consortium, 2006.
- Hinchliffe, Steve, and Kath Woodward (eds). *The Natural and the Social: Uncertainty, Risk, Change*. Routledge, 2000, p. 136.

### **Biography**

With almost 30 years experience in a wide variety of commercial and government software and systems engineering technical and management positions, Robert N. Charette is an internationally acknowledged authority on large-scale software intensive systems development and management. Dr. Charette is best known for his unique integrated approaches to business, financial and technical risk assessment and management.

Charette is the President of the ITABHI Corporation, an international high technology company specializing in enterprise, program and project risk management consulting. Charette is a Fellow of the Cutter Consortium and the Director of its Enterprise Risk Management and Governance Practice, and advisor to the merchant and investment bank Foundation Ventures. He is also the working group chair of the ISO/IEEE 16085 standard on software and systems engineering risk management.