In 2002, Cutter Consortium conducted its first comprehensive survey of the state of risk management practice in the IT community [1]. The survey found that some 86% of organizations responding claimed they were practicing risk management, and 51% of those were practicing it in a disciplined, formal manner. From reports in general software literature, surveys on risk management and its relationship to capturing lessons learned, anecdotal experience, and so on, the practice of risk management seems to have grown both generally and in formality over the past four years. The question is, has it, and if so, by how much? This two-part Executive Report series attempts to answer this question.

We undertook a new survey to find the answer. The results of that survey are presented in Part I (Vol. 3, No. 4) and Part II of this series. Some of the more significant findings are summarized below; the numbers in brackets reflect the 2002 survey results.

- 80% [86%] of the organizations are practicing some type of risk management.
- 66% [51%] that practice risk management are using a formal approach to assessing and managing risk.
- 45% [49%] of the organizations practicing risk management use the traditional definition of risk, while 48% [44%] use a definition of risk that can include positive as well as negative aspects. Some 46% [54%] of the organizations applying formal risk management favor a traditional definition of risk, while 47% [43%] favor using a definition of risk that can include positive as well as negative aspects. This represents a major shift in defining what constitutes a risk for organizations applying formal risk management.
- Only 32% [33%] of the organizations have projects with explicitly defined “drop-dead” thresholds.
- Program/project risk management practices are slowly being integrated into the risk management practices at the corporate level. Some 23% [11%] say that the two are tightly integrated, 46% [41%] say they are loosely integrated, and 30% [48%] say they aren’t integrated at all.
- Some 56% [39%] require a software-oriented risk management process.
- 13% [24%] of those in organizations creating risk management plans never see them.
- 93% [72%] have a process to manage contingencies.
- 35% [48%] of the organizations spend less than 1% of a typical project’s cost on the risk management process, and 69% [77%] spend less than 3%.
- 91% [90%] of the respondents report that managing IT risk is important or very important for achieving project success.
- 60% [56%] believe that the improved ability to reduce
uncertainty is risk management’s main strength. Some 39% [49%] say that the ability to better plan contingencies is the next most important benefit, while 38% [35%] say that improved credibility of project plans produced is the third-highest benefit of risk management.

In 2006, 46% say the top weakness is the difficulty in accurately estimating the level of risk.

41% [52%] say that a specific group is responsible for risk management, while 54% [47%] say an individual within the organization is responsible.

63% [66%] of senior managers are mainly or somewhat supportive of risk management. While 25% [15%] are enthusiastic about risk management, 12% [17%] either ignore it or don’t care about it.

35% [65%] of those organizations practicing risk management do not have any formalized training in risk management.

53% [36%] say that they are capturing lessons learned.

63% [92%] of the organizations are not trying to calculate the ROI of their risk management practice; 37% [76%] believe that they are getting under 50% ROI.

What can we conclude from these findings?

These results indicate that the practice of IT risk management is growing in maturity if not in absolute numbers. The organizations claiming to practice risk management are down slightly from our 2002 survey (80% compared to 86%), but the number of organizations claiming to do formal risk management has increased greatly, from 51% to 66%. If one just compares the 2002 and 2006 results above, a very positive trend in the practice of risk management across the board seems fairly apparent.

There are other indicators of maturation in the practice of risk management as well. Consider the following:

The percentage of individuals claiming to have been performing formal risk management for more than five years has doubled from 16% to 32% during the past four years. This indicates that risk management practice not only has matured but has firmly taken root in a sizable number of organizations.

The major weakness seen in risk management centers on a practice issue (i.e., the problem of estimating risk exposure). This indicates that the focus now is less on getting organizations to use risk management and more on how to apply it. While gaining organizational buy-in is still a major issue for organizations practicing informal risk management, it has become a nonissue for organizations practicing formal risk management.

There is the almost universal application of contingency management. At the very least, it indicates that some type of risk assessments are being performed by organizations, even if it isn’t the practice of continuous risk management.

Of course, these positive indicators must be tempered with the knowledge that the survey findings for the most part focus on organizations that have indicated that they use risk management. They don’t look so positive if we compare the numbers against all of our survey respondents. Furthermore, significant weaknesses in risk management practice that we found in 2002 still exist today. For instance, risk acceptability is still not routinely defined. If you cannot define what is and is not acceptable, how can an organization do effective risk management?

Has IT risk management reached the tipping point, that is, is it here to stay as a routine practice? For those who are practicing risk management, formally or informally, the answer appears to be yes. But the dip in the percentage of total organizations saying they use risk management may portend something different. Maybe four years from now — in 2010 when we do our next survey — we will have a better answer to that question.

REFERENCE