Risk Management 2006: A Comprehensive Survey (Part I)

by Robert N. Charette, Fellow, Cutter Consortium

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 decided to use the 2002 survey as a benchmark. In this way we could compare and contrast the current state of the practice with what we found four years ago. Therefore, to ensure consistency, the questions you find in this two-part Executive Report series are nearly identical to those we asked in 2002, with the exception being that we simplified the wording in a couple of questions as well as added a few clarifying questions to improve our understanding of the responses we received.

In 2002, we compared organizations that use formal approaches to risk management against those that use informal approaches, and we do so again in this series. We also look at how different levels of management view risk management as well as how risk management is practiced in different geographical areas and industry sectors.

The first half of the results are presented in the accompanying Executive Report and include an examination of the survey responses regarding the risk management experience of our participants, their principles, areas in which risk management is needed, and the software processes surrounding the field. Part II (to be published next month) will explore the second half of the data.

SURVEY DEMOGRAPHICS

We conducted our risk survey during the early months of 2006. A total of 182 persons in various IT positions responded to more than 50 risk management–related questions. To gain some perspective on our 2006 survey, the following describes the general demographics:

- 60% of our survey respondents are involved in management positions, with 19% being senior managers or policy makers. More managers responded to this survey than in 2002.

- Our survey respondents come from a wide variety of international organizations: North America (46%); Europe (24%); Asia (10%); Australia/Pacific (10%); India (3%); South

Cutter Consortium Enterprise Risk Management & Governance Executive Summary Vol. 3, No. 4
Company represented in the survey come from 25 different industries, ranging from computer software to telecommunications to financial services to healthcare. National, state, and local governments are also represented.

The size of the organizations represented ranges across the spectrum from large to small. Respondents come from companies having corporate revenues in four categories: those with revenues of less than US $5 million (31% of the respondents); those with revenues of $5 million to $100 million (29%); those with revenues of $100 million to $1 billion (16%); and those with revenues of more than $1 billion (24%).

Annual IT expenditures by the organizations our respondents work for are generally equally as spread out as annual revenues.

Overall, the survey demographics are very similar to those of our 2002 survey.

**KEY FINDINGS**

Some of the more significant findings discussed in Part I 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. 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.
- A variety of risk management techniques are being used by organizations. Cost-benefit analysis is the most popular technique and is used by 60% [61%] of the organizations; 45% [35%] use scenarios; 41% [41%] use threat analysis; 40% [37%] use questionnaires; 33% [18%] use risk taxonomies; 23% [23%] use decision trees; and 21% [21%] use network/PERT charts.

**CONCLUSION**

While it is dangerous to extrapolate from just two data points from two different sample pools, my impression of the data is that it indicates 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% down from 86%), but the number of organizations claiming to do formal risk management has increased greatly, from 51% to 66%. If one compares just the 2002 and 2006 results above, a very positive trend in the practice of risk management across the board seems fairly apparent. Stay tuned for Part II, where we will explore further details of the survey.

**REFERENCE**


---

**About the Service**

**ENTERPRISE RISK MANAGEMENT & GOVERNANCE ADVISORY SERVICE**

**SENIOR CONSULTANTS**

Robert N. Charette; Director; Steve Andriole; Robert D. Austin; Edmund H. Conrow; Christine Davis; Tom DeMarco; Lynne Ellyn; Kerry Gentry; Sebastian Konkol; Steve Kursh; Lynne Nix; Carl Pritchard; Mark Seiden; Scott Stirbny; William Zucker

**FOR MORE INFORMATION**

For more information on Cutter Consortium’s ERM&G Advisory Service or its other services, contact: Tel: +1 781 648 8700 or, within North America, +1 800 964 5118; Fax: +1 781 648 1950 or, within North America, +1 800 888 1816; E-mail: sales@cutter.com.

The Executive Summary is a supplement to the ERM&G Advisory Service’s Executive Report. ©2006 by Cutter Consortium. All rights reserved. Unauthorized reproduction in any form, including photocopying, faxing, image scanning, and downloading electronic copies, is against the law. Reprints make an excellent training tool. For information about reprints and/or back issues of Cutter Consortium publications, call +1 781 648 8700 or e-mail service@cutter.com.

©2006 by Cutter Consortium