

# Risk Management (II)

Source: **PricewaterhouseCoopers**  
Author Name: **CFOdirect Network**  
Published: **12.13.06**

## Background

The term **risk management** is applied in a number of diverse disciplines. People in the fields of statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory, to name a few, have been addressing the field of risk management.

Kloman summarized the meaning of risk management in the context of a number of different disciplines in an article for *Risk Analysis* :

"What is risk management? To many social analysts, politicians, and academics it is the management of environmental and nuclear risks, those technology-generated macro-risks that appear to threaten our existence. To bankers and financial officers it is the sophisticated use of such techniques as currency hedging and interest rate swaps. To insurance buyers and sellers it is coordination of insurable risks and the reduction of insurance costs. To hospital administrators it may mean 'quality assurance.' To safety professionals it is reducing accidents and injuries."

Kloman Paraphrase of Rowe

Risk management is a discipline for living with the possibility that future events may cause adverse effects.

## SEI Risk Statement

For a risk to be understandable, it must be expressed clearly. Such a statement must include a description of the current conditions that may lead to the loss

## Risk Example

A company has introduced object-oriented (OO) technology into its organization by selecting a well-defined project "X" with hard schedule constraints to pilot the use of the technology. Although many "X" project personnel were familiar with the OO concept, it had not been part of their development process, and they have had very little experience and training in the technology's application. It is taking project personnel longer than expected to climb the learning curve. Some personnel are concerned, for example, that the modules implemented to date might be too inefficient to satisfy project "X" performance requirements.

The risk is: Given the lack of OO technology experience and training, there is a possibility that the product will not meet performance or functionality requirements within the defined schedule.

### **Non-Risk Example**

Another company is developing a flight control system. During system integration testing the flight control system becomes unstable because processing of the control function is not quick enough during a specific maneuver sequence.

The instability of the system is not a risk since the event is a certainty - it is a problem.

### **Continuous Risk Management Example**

When using Continuous Risk Management, risks are assessed continuously and used for decision-making in all phases of a project. Risks are carried forward and dealt with until they are resolved or they turn into problems and are handled as such.

### **Non-Continuous Risk Management Example**

In some projects, risks are assessed only once during initial project planning. Major risks are identified and mitigated, but risks are never explicitly looked at again.

This is not an example of Continuous Risk Management because risks are not continuously assessed and new risks are not continuously identified.

### **Software Risk Evaluation**

The SEI Software Risk Evaluation (SRE) Service is a diagnostic and decision-making tool that enables the identification, analysis, tracking, mitigation, and communication of risks in software-intensive programs. An SRE is used to identify and categorize specific program risks emanating from product, process, management, resources, and constraints. The program's own personnel participate in the identification, analysis, and mitigation of risks facing their own development effort.

An SRE provides a program manager with a mechanism to anticipate and address program risks. The SRE introduces a set of activities that, when initiated, begin the process of managing risk. These activities can be integrated with existing methods and tools to enhance program management practices.

For more information, see Software Risk Evaluation Service Web page.

## **Risk Process Check**

A Risk Process Check is the SEI's most recently developed risk management service. It is combination of tutorial, survey instrument, interviews, and feedback session conducted on-site to determine how effective the project or program's risk management process is. It is based on the SEI's Seven Principles of Risk Management , and, being principle-based rather than model-based, it can evaluate any risk management process, whether it follows the guidelines of the SEI's Continuous Risk Management course or some completely different model.

The Risk Process Check has been used on one major DoD program (DoD program office, prime contractor, and two subcontractors to the prime) and two contractor organizations to a non-DoD government agency. There are many areas of opportunity to refine and further define this service with the SEI.

## **Continuous Risk Management Guidebook**

The Continuous Risk Management Guidebook was written with professionals in mind who are directly involved in software-intensive projects (program managers, lead engineers, software engineers, etc.). It may also be of interest to professionals from other disciplines (e.g., quality assurance, hardware engineering, testing) involved in software-intensive projects, and sponsors, change agents, technology transition agents, and software engineering process group members in organizations that want to improve.

The *Continuous Risk Management Guidebook* describes the underlying principles, concepts, and functions of risk management and provides guidance on how to implement it as a continuous practice in your projects and organization. Risk management can be used to continuously assess what can go wrong in projects (i.e., what the risks are), determine which of these risks are most important, and

implement strategies to deal with these risks. The guidebook is based on proven practices confirmed through research, field testing, and direct work with clients.

The *Continuous Risk Management Guidebook* was developed to help a project or organization establish continuous risk management as a routine practice and then continue to improve this process. It is organized so that different users can read different parts of the book and get different benefits. For example, technical managers and lead engineers can read the book to learn how to build a risk management process that is tailored to their specific project or organization; software engineers can use it to understand how to perform the risk management methods and use the tools described in the guidebook; and change agents (such as members of software engineering process groups) can read it to understand why continuous risk management should be used and how to get projects to tailor it and start using it. In addition, all users of this guidebook will gain a greater understanding of continuous risk management.

Although the Guidebook deals primarily with performing continuous risk management in a software development environment, it can easily address systems, hardware, and other domains.