Risk Management for IT and Software Projects

DR. E. WALLMÜLLER
Qualität und Informatik www.itq.ch, Zürich

Abstract: Risk Management can be defined as a systematic process for identifying, analyzing and controlling risks in projects or organizations. Definitions and illustrations of risks are given especially by a list of ten risk factors, which occur most frequently in IT and Software projects.
For complex, high-risk projects it is very useful to implement a formal risk-management process, supported by effective methods in the individual process steps. As variants, risk-management processes according to Barry Boehm, Ernest Wallmüller and Jyrki Kontio are presented.
The importance of a sound operational preparation of each step of the risk-management process is emphasised and illustrated by examples.

Keywords: Risk Management Process, Riskit, Risk Management, Quality Management, Identification of risks, Analysis of risks, Control of risks, Monitoring of risks, Project risks, Risk scenario, Risk definition

1 Motivation

In order to increase the likelihood of a project reaching a successful conclusion, the risks or potential problems for a project need to be identified at an early stage and appropriate countermeasures developed. Tom Gilb put it in a nutshell with the following words: "If you don’t actively attack the risks, the risks will actively attack you." Experience shows [Boeh89] that handling risks proactively, as is the case with risk management, is less expensive than correcting problems in the aftermath.

2 Background

Risk management has been around for some time. The word "risk" stems from the Italian verb "risicare". The science of risk management was developed back in the sixteenth century

during the Renaissance, a period of discovery. The theory of probability, which is the core of risk management, was developed to help better estimate people's chances in games.

What is a risk? This question can best be answered using an example from everyday life. All cigarette packs are marked with warnings such as "Smoking is dangerous to your health" or "Smoking causes cancer". If one analyses these statements, one sees that they describe a cause (smoking) of a problematic situation (cancer occurs) and its impacts (shortening of life).

There are many definitions of the term "risk" but no generally accepted one. All definitions implicitly include two characteristics: uncertainty (an event may or may not occur) and loss (an event has undesired effects). This is demonstrated by the following examples:

- used in nouns, the word "risk" indicates that somebody or something is subject to a danger or certain dangers;
- risk is the potential for the occurrence of undesired, negative consequences of an event [Rowe88];
- risk is the possibility of suffering losses, damage, disadvantages or destruction [Webs81].

Based on Webster's description of "risk", we shall use the following definition:

risk is the possibility of suffering losses due to an event that will quite probably occur.

According to [Kont97], a risk can be illustrated using "risk scenarios" containing the following elements:

- a risk factor is something than influences the probability of a negative event occurring;
- a risk event is the occurrence of a negative incident or the discovery of information revealing negative circumstances;
- a risk reaction is an action which can be carried out when a risk event occurs; and
- a risk effect is the impact of a risk event on the project.

A risk scenario is a chain consisting of a risk factor, risk event, risk reaction and risk effects. The example given in Figure 1 includes the following risk scenario: "The database release is still in the beta-test phase. Problems could occur with the database integration. If so, a database expert might have to be called in. This would cause additional project costs totaling DM 20,000."

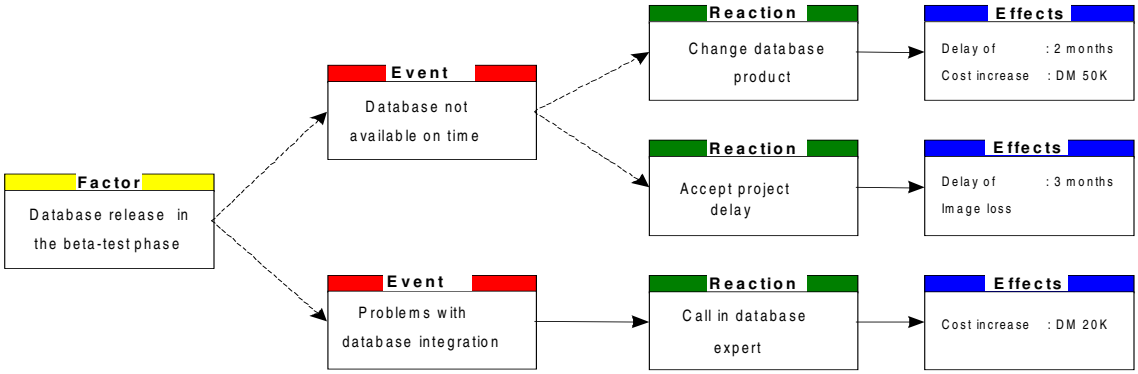

Figure 1: Example of a risk scenario

As opposed to purely textual descriptions of risks, risk scenarios offer the advantage that the risks can be divided into individual elements, making it possible to define targeted measures. On the one hand, attempts can be made to eliminate the risk factor or reduce the probability of the risk event occurring. This type of measure is referred to as a "preventive measure". On the other hand, additional, more effective risk reactions can be defined or the risk effects reduced. These measures are known as "precautionary measures".

So risk management can be defined as follows:

> risk management is a systematic process for identifying, analyzing and controlling risks in projects or organizations.

3 Example Risks

The literature on this subject describes a plethora of risks which can occur in software development. Many sources suggest measures for decreasing the probability of these risks occurring. According to [Boeh98], there are ten risk factors which occur most frequently (see Figure 2).

Risk factor	***Preventive measures***
1. Human error on part of staff	Employ the best people; rewards; team formation; training; peer reviews; adapt process to available know-how
2. Unrealistic schedule and budget	Business-case analysis; incremental development; reuse of software; modification of schedule and budget
3. Standard software,	Benchmarking; prototyping; review of reference

external components (inexperience, incompatibility, etc.)	installations; compatibility analysis; review of suppliers
4. Requirements and developed functions do not match	Win-win agreements between parties concerned; business-case analysis; prototyping; application description in early phases
5. User interfaces do not fit needs	Prototyping; development of scenarios; description of users
6. Inadequate architecture, performance, quality	Simulation; benchmarking; modeling; prototyping; tuning
7. Constant alteration of requirements	Increased threshold for changes; information-hiding; incremental development; change-management process; change control board
8. Problems with legacy systems	Design recovery; restructuring
9. Problems with tasks performed externally	Audits; parallel design or prototyping by several suppliers; team formation
10. Overestimation of own IT capabilities	Technical analysis; cost/benefit analysis; prototyping

Figure 2: Boehm's ten risk factors

4 The Risk-Management Process

Risk management has always been a part of software development. Project managers and other project staff can usually identify risks intuitively and deal with them. However, as the risks described in Figure 2 show, that is not always enough. A formal risk-management process, supported by effective methods in the individual process steps, needs to be implemented for complex, high-risk projects. The following three examples of risk-management processes will be described in the sections below:

- the first formal risk-management process in software development, described by Barry Boehm in 1989 [Boeh89];
- a risk-management process, defined in [Wall99] as an integrated part of project management; and
- a risk-management process which places great emphasis on the project's goals and stakeholders when analyzing risks and their effects. This process was described by Jyrki Kontio in 1997 [Kont97].

Apart from [Boeh89], there are numerous other standard works on risk management, for example [Char89], [Doro96] and [Jone94].

4.1 Boehm's Risk-Management Process

Risk management was introduced as an explicit process in software development in the 1980s. The father of software risk management is considered to be Barry Boehm, who defined the risk-driven spiral model [Boeh88] - a software-development lifecycle model - and then described the first risk-management process [Boeh89]. Most of the processes defined since then stem from his basic process. His risk-management process consists of two sub-processes, "risk assessment" and "risk control" (see Figure 3).

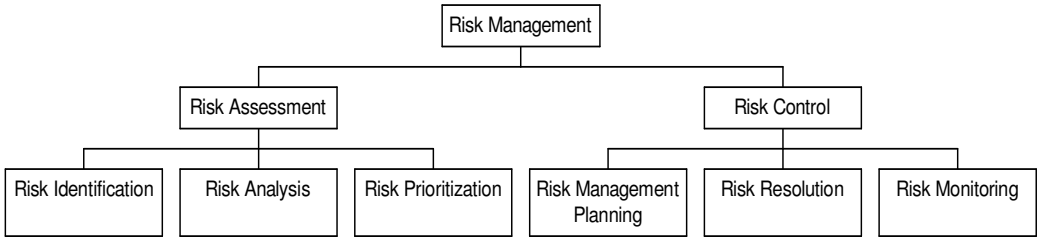

Figure 3: Boehm's risk-management process

The risk-identification process entails listing all conceivable risks to the project. Creative methods, e.g. brainstorming, and analytical methods, e.g. a risk checklist, can be used here. The risk analysis evaluates the risks. This involves determining the probability of occurrence and the possible negative effects for each risk. The risk-prioritization stage is used to specify the sequence in which the risks are to be dealt with. To this end, the losses caused when risk events occur are evaluated.

The process of risk-management planning involves specifying measures intended to reduce the probability of risk events occurring or to diminish the negative impacts following the occurrence of the risk event. Risk resolution is the step of the process where the defined measures are carried out. Risk monitoring keeps track of the efficiency of the measures implemented. In order to do this effectively, risk-monitoring metrics should be specified in the risk-management planning stage and the related data should be captured during the risk-resolution process.

4.2 Wallmüller's Risk-Management Process

[Wall99] describes a process whereby the risk-management activities are conducted by the project team at the same as the cost-, time-, quality- and requirement-management activities.

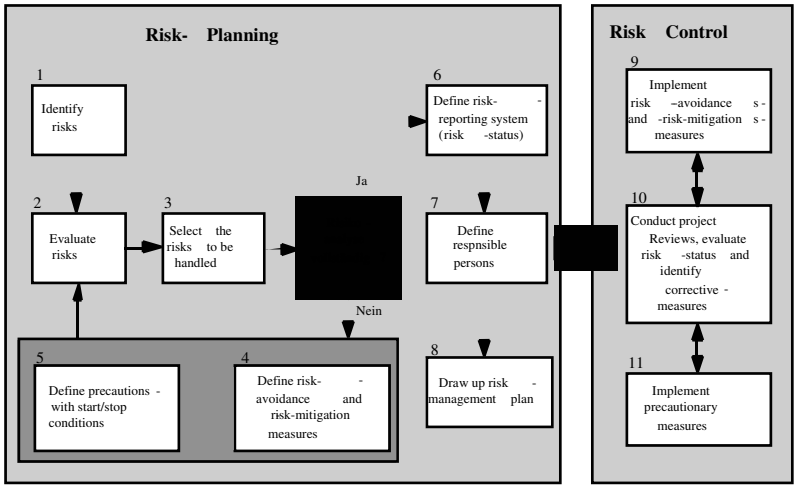

Figure 4: Wallmüller's risk-management process

Unlike Boehm's process, this is a sequence-oriented process (see Figure 4). It consists of a risk-planning part (steps 1–8) and a risk-control part (steps 9–11). The risk-planning part starts in the project-preparation and planning phase before the actual project kick-off. The process runs full circle at least once in a project phase. This is also referred to as continuous risk management.

Many activities are the same as in Boehm's process. A significant new component is the assignment of different risk-management roles. The project manager determines the general risk-management strategy, including the appointment of the risk manager and assignment of risk-management responsibilities. The project manager works with the risk manager and the project team (clients, suppliers and subcontractors) in order to identify risks and define probabilities and impacts. He or she plans and approves the implementation of financial, time-related and technical preventive and precautionary measures, monitors and establishes reporting procedures.

The project team identifies risks within its area of responsibility, appraises probabilities and impacts, prioritizes risks, identifies preventive and precautionary measures, reports on the

status of risks, evaluates the efficiency of the preventive and precautionary measures and implements, if necessary, the precautionary measures.

The risk manager supports the project team in the risk-planning and risk-control processes, implements the risk-management plan, organizes and administrates risk-status reports, evaluates new risks, checks the effectiveness of current risk plans and of the implementation of precautionary measures.

4.3 Kontio's Risk-Management Process (Riskit)

Riskit is a goal-oriented and stakeholder-oriented style of risk management [Kont97]. Riskit distinguishes between two phases: the initialization phase and the risk-analysis cycle. The latter has many parallels with Boehm's basic process and Wallmüller's risk-management process. This phase will thus not be described in detail here. In the initialization phase the foundations upon which the risk-management process is performed are laid.

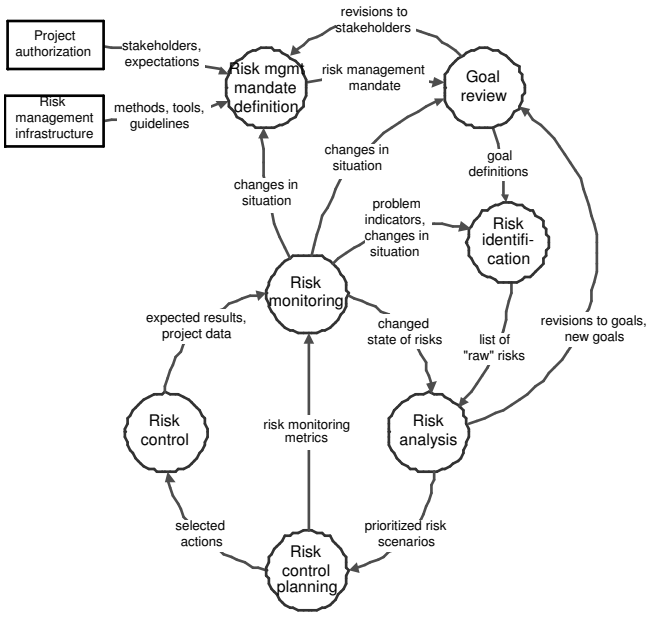

Figure 5: Kontio's risk-management process (Riskit)

The aim of the first process step, "Risk-management mandate definition", is to establish a risk-management procedure for the project in consultation with all parties involved (e.g. project manager, risk manager and project team) (Figure 5). The risk-management process must be adjusted to the complexity and riskiness of the project. In the case of small projects, where no major risks are to be expected, it usually suffices to discuss risks at the project-management meetings from time to time. In complex, high-risk projects (e.g. when new development methods are used), a formal risk-management process, supported by well-developed methods, is required. The results of this first process step are:

- risk-management targets, methods and tools;
- a defined time frame for the analysis cycles (e.g. once a month);
- a definition of risk categories which are not to be considered (e.g. marketing risks);
- risk-management roles and tasks;
- communication mechanisms and reports; and
- project stakeholders and their expectations vis-à-vis the project results.

In particular, it is the consideration given to stakeholders that distinguishes Riskit from other risk-management methods. This concept is based on the idea that different stakeholders have different goals and expectations for the project. Consequently, the second process step, "Goal review", examines the project targets and formulates them in as measurable a form as possible. It also analyses which goals are how important for which stakeholder.

Goals and stakeholders place a crucial role in the "Risk analysis" step. Each risk is analyzed to determine its impacts on the project goals. These impacts are described in as measurable a form as possible (e.g. project delayed by three months = budget exceeded by $ 50,000). Since the "Goal review" step defines in advance which goal is important for which stakeholder, it is then possible to estimate who will incur the largest loss if a risk event occurs. These analyses are also of benefit when specifying measures.

5 Risk-Management Methods

In order to conduct a risk-management process in a systematic manner, it is important to have well-developed methods for each process step. To list all of the methods described in the literature would be to exceed the limits of this article so only a few examples will be given. An extensive assortment of risk-management methods can be found in [Doro96].

5.1 Risk-Identification Methods

As a rule, two types of methods are used for identifying risks. Firstly, brainstorming methods, which activate the project staff's creativity. And secondly, there are a variety of risk checklists comprising the typical project risks. These checklists can be used in group or one-to-one discussions to identify risks. One very well-known checklist is the "Taxonomy-Based Questionnaire" [Carr93], containing 194 questions, which are divided into various categories, i.e.:

- Product Engineering (requirements, design, code and unit test, integration and test, engineering specialties)
- Development Environment (development process, development system, management process, management methods, work environment)
- Program Constraints (resources, contract, program interfaces)

Figure 6 shows an extract from a checklist which this author uses.

Schedule/ Location

- Time frame
- Geography
- Location
- Real Schedule vs. Bid Schedule

Technical

- Requirements
- Prototypes
- Tools
- Functionality
- Technical Performance
- Available and Future Technologies
- Architectures
- Integration
- Support Service (Training, Rollout , Installation)
- Baseline Management
- Unproven Hardware

Subcontractors

- Statement of Work
- Price
- Terms & Condition
- Resources /Experiences
- Subcontractor Management
- Quality Control
- Invoicing
- Alternate Sources

Contract

- Change Control Process
- Terms & Condition /Payment Plan
- Acceptance Criteria
- Statement of Work /Deliverables

Resources

- Bid/Proposal Resources
- Skills /Qualification /Capabilities
- Implementation Resources
- Facilities (e.g. Space , Equipment)
- Logistics

Innovation Projects

- Market Knowledge
- Transformat ion Client Needs
- Speed Idea => Product
- Changes of Requirements
- Team
- Management Support /Commitment
- Number of Projects in Parallel

Figure 6: Risk checklist

5.2 Risk-Analysis Methods

One of the first steps in a risk analysis is to describe the risk in detail. An example form for this purpose can be found in [Doro96]. Based on this form, a risk description contains the following information , some of which is not gathered until the control measures or the monitoring phase is planned:

- unique risk title,
- identification date,
- formal description of the risk using risk factor, risk event and risk effect,
- context description containing additional information in text form,
- person who identified the risk,
- priority,
- probability of a risk event occurring,
- degree of impact (risk effect),
- time at which the risk event is likely to occur or at which measures have to be taken,
- classification,
- responsible person,
- strategy aimed at reducing the probability of the risk event occurring or at avoiding the risk,
- action plan should the risk event occur,
- status and date when the status was last recorded,
- person who accepted the risk, e.g. project manager,
- conclusion date and
- reason for conclusion.

The risks can be prioritized based on qualitative criteria with the help of a risk portfolio. With this method, the probability of the risk event occurring and the degree of impact are rated as "low", "medium" or "high". Thus, three priority categories can be defined:

- high-priority risks (A quadrant) are those which are rated as "high" for one parameter and at least "medium" for the other;
- low-priority risks (C quadrant) are those rated as "low" for one parameter and at the most "medium" for the other; and
- the other risks are assigned medium priority (B quadrant).

Presenting the risks in the form of a portfolio chart provides a good overview of the priorities which are important for risk resolution (see Figure 7).

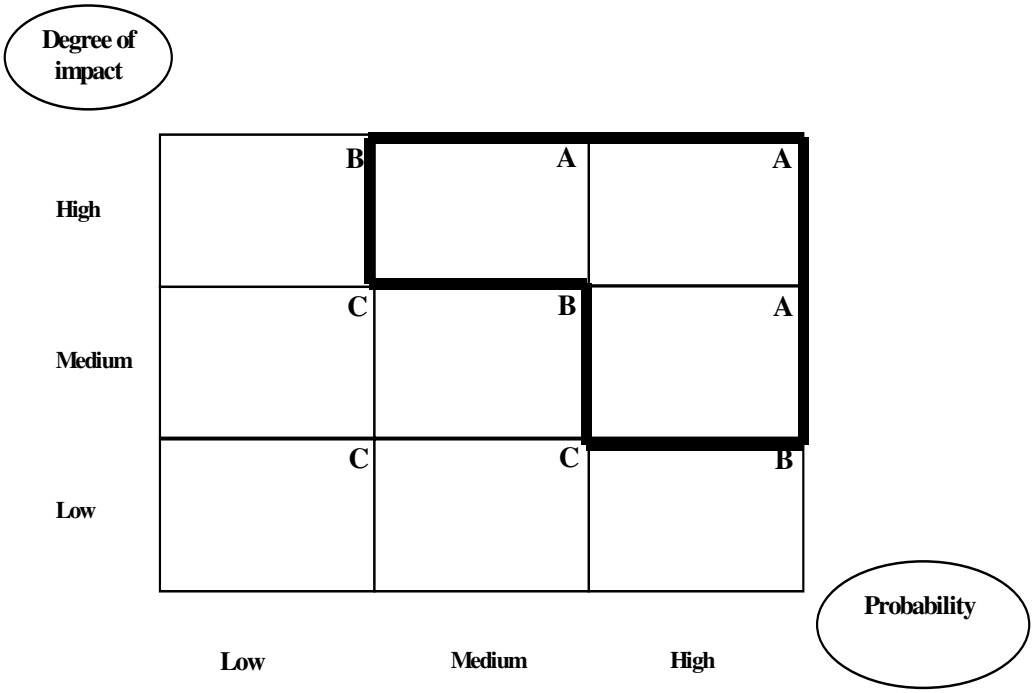

Figure 7: Risk portfolio

A good means of evaluating risks quantitatively and prioritizing them is the risk-exposure method [Boeh89]. With this method, the probability of a risk event occurring is given as a value between 0 and 1 and the impact of the risk is given as a measurable value. The risk exposure is calculated as follows:

Risk exposure = Probability * Impact

Thus, an impact in the form of a $ 100,000 loss with a 20% probability of occurrence results in the following risk exposure:

Risk exposure = 0.2 * $ 100,000 = $ 20,000.

5.3 Methods for Planning Control Measures

Once a risk has been analyzed, one or several strategies should first be defined as to how the project members should handle the risk. [Hall98] cites the following fundamental risk strategies:

- risk acceptance: no action is taken to counter the risk, the impacts are accepted. This strategy can be opted for if the impacts are minor or if the effort required to implement the measures exceeds the impacts of the risk events;
- risk prevention: attempts are made to prevent the risk event from occurring at all. This strategy is chosen when the impacts are serious;
- anti-risk measures: targeted redundancies (e.g. duplicate processors and disks in tandem systems);
- risk mitigation: this strategy reduces the probability of the risk event occurring or the degree of the impacts;
- risk research: additional information is obtained. This strategy is opted for if the individual risk elements are not sufficiently transparent;
- risk reserves: reserves are included in the project budget or time frame. This strategy is chosen when there is great uncertainty in the project;
- risk transfer: the risk is passed on to other persons, groups or organizations. This strategy is used when others control the risk and the measures to be taken.

Once the risk strategy has been selected, a risk-management plan can be devised. This plan is used to add information to the risk description, e.g. person who accepted the risk, person responsible, preventive measures and precautionary measures. [Jone94] contains an extensive assortment of possible risk measures.

5.4 Risk-Monitoring Methods

In order to monitor the current status of the risks and the measures defined, metrics can be specified for the risks. These metrics can be quantitative, such as the probability of occurrence or effort for and cost of control measures. But they can also be qualitative, e.g. an appraisal of project staff's motivation.

Another monitoring method is to use triggers, which are threshold values for metrics which trigger measures when reached.

Whereas metrics and triggers are only used in well-developed risk-management processes, risk reports are almost always used as a means of monitoring. The literature refers to many different types of report, e.g. the risk description, which is updated when risk measures are completed, or the risk table (see Figure 8).

Example I

Project:	Major Systems Integration
Status Date:	September 1, 1993
Origination Date:	March 20, 1993
Risk Number:	1
Risk Title:	System Interface Definition
Functional Area:	Systems Engineering
Responsible Person:	John Systems
Critical Milestone:	System Requirements Review (SRR)
Risk State:	Active Risk
Risk Probability:	40
Cost Impact:	$ 1,500,000
Schedule Impact:	unknown
Performance Impact:	non-compliance
Spec/WBS Ref:	Sys Spec-3.3.1.1/AA200

Risk Definition:

The client's system specification is incomplete, specifically in the area of system interfaces.

Example II

Risk Avoidance/Mitigation Status:

Three primary risk avoidance/mitigation efforts are underway and include active client participation in the requirements validation effort, the establishment of an interface control working group, and the creation of interface specifications and interface control documents for each interface. Current status is as follows:

1. Requirements validation is in process. The client is actively participating and supporting this endeavor. Systems engineering is assigned to track this effort.
2. An interface control working group has been established with members from all client user groups and end customers. All major interface requirements have been identified.
3. Six of the eight interfaces have a requirements specification documented. The requirements for the remaining interfaces will be defined prior to SRR.

Risk Contingency Plans Status:

The contingency plans include utilizing a phased implementation and designing in flexibility in the overall system design for easy accommodation of phase II requirements. Also optionally obtaining schedule and/or milestone payment relief from the client.
An acceptable alternative phased implementation schedule has been created and approved by the client. The implementation of phase II applications will be delayed approximately three months. A separate phase II SRR will be held. This delay will add approximately $ 100K to our cost. Neither contingency plan is currently implemented. Implementation will be initiated if the remaining interfaces are not firmly established and defined at the System Requirements Review (SRR).

Figure 8: Examples of risk reports

6 The Importance of Risk Management for Quality Management

In many software projects, key business processes are optimized and the supporting software-system environment is redesigned. These projects are complex in that they have a complex structure and generate complex software systems. Migration of different legacy systems and integration of systems into an extensive IT system environment also raise the complexity.

Project-planning and quality-planning as well as problem and risk management can be used to define and prioritize QM measures. Risk management in particular is an ideal process for focussing the QM measures on the critical aspects of the project.

7 Conclusion

Risk Management is a practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision making to

- assess continuously what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks

There will be a cultural shift from "fire-fighting" and "crisis management" to proactive decision making that avoids problems before they arise. Anticipating what might go wrong will become a part of everyday business, and the management of risks will be as integral to program.