Presented at the SIGSOFT'98 Sixth International Symposium on the Foundations of Software Engineering (FSE-6), November 3-5, 1998

Experiences in improving risk management processes using the concepts of the Riskit method

Jyrki Kontio*
Nokia Telecommunications
IP Networking
P.O.Box 315
00045 NOKIA GROUP, Finland
Tel: +358-9-5116-3233
jyrki.kontio@ntc.nokia.com

Gerhard Getto
Daimler-Benz AG
Research and Technology
P.O.Box 2360
89013 Ulm, Germany
Tel: +49-731-505-2872
getto@dbag.ulm.DaimlerBenz.com

Dieter Landes
Daimler-Benz AG
Research and Technology
P.O.Box 2360
89013 Ulm, Germany
Tel: +49-731-505-2872
landes@dbag.ulm.DaimlerBenz.com

1 ABSTRACT

This paper describes experiences from two organizations that have used the Riskit method for risk management in their software projects. This paper presents the Riskit method, the organizations involved, case study designs, and findings from case studies. We focus on the experiences and insights gained through the application of the method in industrial context and propose some general conclusions based on the case studies.

1.1 Keywords

risk management, project management, empirical study

2 INTRODUCTION

All software development projects involve risks and all experienced project managers do pay attention to the uncertainties involved in software development. Naturally, there are individual differences on how well different project managers deal with risks. As few organizations apply systematic, documented risk management methods, most project managers rely on intuition – and luck – instead of managing risks systematically and consistently. Given that most software projects are complex and involve various types of risks and commitments, leaving risk management up to the individual intuition and initiative may sometimes work but is a poor substitute for a systematic, professional and consistent approach for risk management.

This paper presents experiences from situations where more systematic risk management principles were introduced into projects using the Riskit method [19].

3 PRESENTATION OF RISKIT METHOD

Riskit is a comprehensive risk management method that is based on sound theoretical principles and thus it avoids many of the limitations and problems that are common to many other risk management approaches in software engineering. As the Riskit method has been extensively presented in other publications [11,19-22], we present here only the highlights and main principles of the method. While the Riskit method can be applied in many other domains as well -- such as business planning,, marketing, and technology selection -- it has been originally developed for software development projects and its main features correspond to the risk management concepts and practices required in software projects, as discussed in the following.

3.1 Complete Process Definition

The Riskit method has a comprehensive process definition that supports risk management activities throughout the project [19]. The Riskit process is similar to many other risk management process descriptions with some special characteristics:

- Full operational definition of the process as well as guidelines available for using the associated techniques.
- A specific step where the risk management mandate is defined, i.e., the scope, focus, authority and procedures of risk management are explicitly addressed and defined.
- A specific step for identifying and defining the goals and stakeholders for the project, including means to keep goal definitions up-to-date.
- Adaptation of utility theory to the assessment of risk in software engineering
- A sound approach for prioritizing risk information when only ordinal level metrics are available.

* Jyrki Kontio is also affiliated with Helsinki University of Technology, Dept of Computer Science and Engineering, Laboratory of Information Processing Sciences, P.O. Box 1100, FIN-02015 HUT, Finland, tel: +358-9-451-4852 , E-Mail: jyrki.kontio@cs.hut.fi

The Riskit process overview is presented in Figure 1 as a dataflow diagram. The main processes are also described in Table 1. More detailed process description is available in a separate report [19].

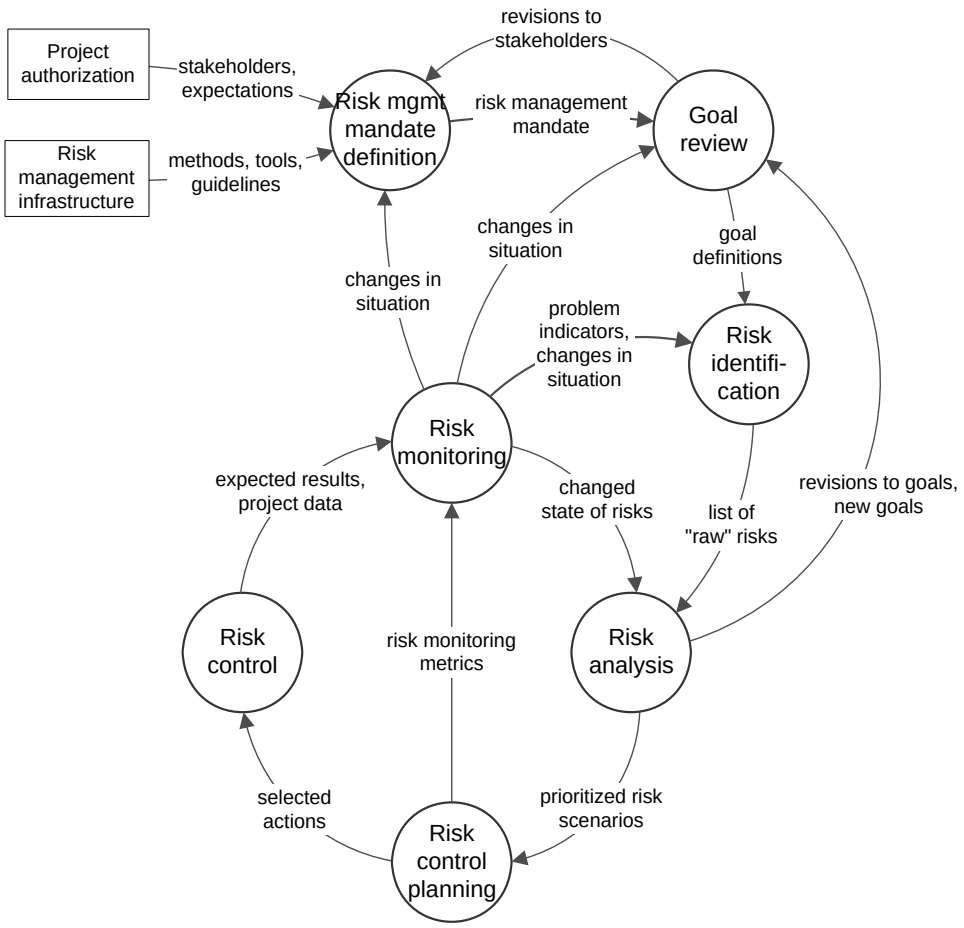

Figure 1: The Riskit risk management cycle

3.2 Goals and Stakeholders

Most risk management methods do not explicitly support different stakeholder perspectives [9,12,16-18,23] and those that do, often limit the number of stakeholders and assume that consensus can be reached [24]. Boehm's Win-Win approach is the only major risk management approach that focuses on stakeholder goals [6]. The Riskit method extends Boehm's approach by maintaining links between risks and stakeholders explicitly. These links are visualized in Figure 2. The Riskit method contains templates and guidelines on how to identify, analyze and document all the elements listed in Figure 2.

When risk scenarios are defined, their impact to project is described through the stated project goals. This allows full traceability between risks and goals and on to stakeholders: each risk can be described by its potential impact on the agreed project goals, and each stakeholder can use this information to rank risks from their perspective.

Riskit step	Description	Output
Risk management mandate definition	Define the scope and frequency of risk management. Recognize all relevant stakeholders	Risk management mandate: why, what, when, who, how, and for whom
Goal review	Review the stated goals for the project, refine them and define implicit goals and constraints explicitly. Analyze stakeholders' associations with the goals.	Explicit goal definitions
Risk identification	Identify potential threats to the project using multiple approaches.	A list of "raw" risks.
Risk analysis	Classify and consolidate risks. Complete risk scenarios for main risk events. Estimate risk effects for all risk scenarios Estimate probabilities and utility losses of risk scenarios.	Completed Riskit analysis graphs for all analyzed risks. Ranked risk scenarios.
Risk control planning	Select the most important risks for risk control planning. Propose risk controlling actions for most important risks. Select the risk controlling actions to be implemented.	Selected risk controlling actions.
Risk control	Implement the risk controlling actions.	Reduced risks.
Risk monitoring	Monitor the risk situation.	Risk status information.

Table 1: Overview of outputs and exit criteria of the Riskit process

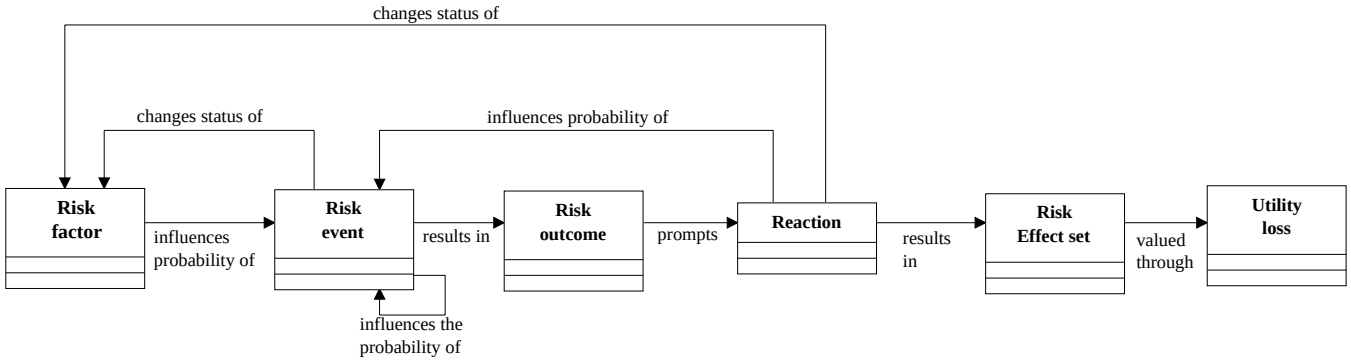

Figure 3: A conceptual view of the elements in the Riskit analysis graph

3.3 Definition of Risk

The Riskit method supports unambiguous definition for risks. The common definition of risks, either by dictionaries or every-day usage, associate several different meanings to risk. It can refer to a possibility of loss, the actual loss that would result if the risk occurs, a factor or element that is associated with a threat, or a person that contributes to the possibility of loss [19]. While it is sometimes necessary to refer to any of these aspects of risk on an abstract level, we

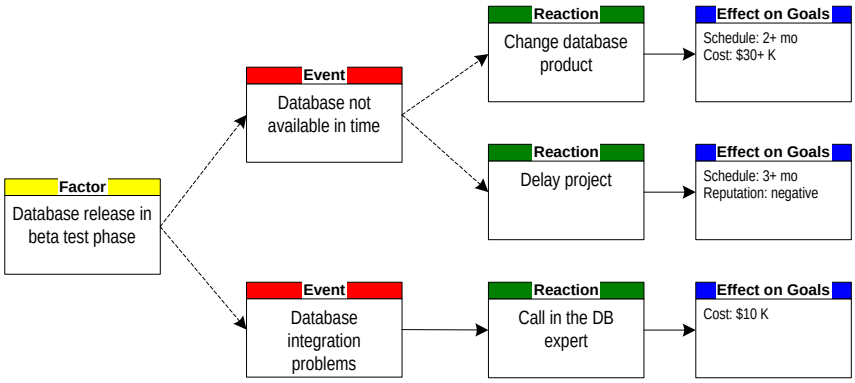

Figure 4: Example of the Riskit analysis graph (risk scenarios)

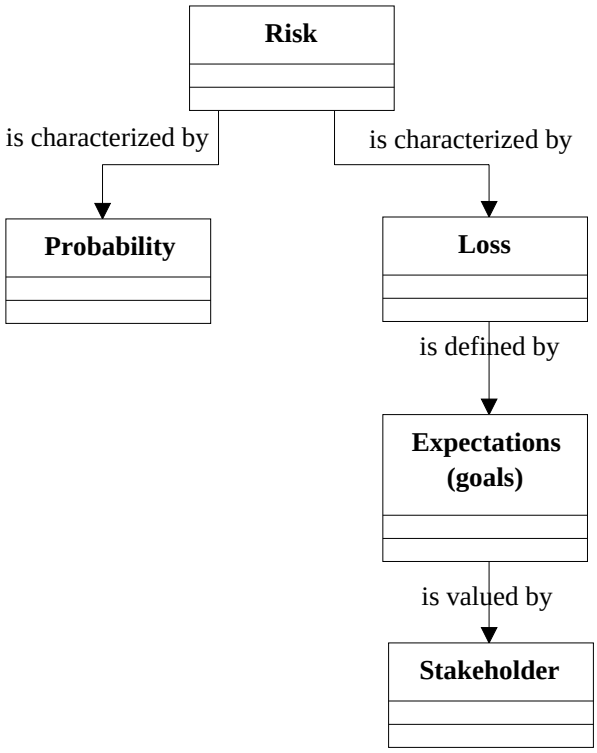

Figure 2: Definition of risk in the Riskit method

believe that a more analytical discussion on risk requires more precise terms. Thus, in the Riskit method the risk itself is defined on a general level as *a possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility.*

The *Riskit analysis graph* is a graphical formalism that is used to define the different aspects of risk more formally. The Riskit analysis graph can be seen both as a conceptual template for defining risks, as well as a well-defined graphical modeling formalism.

The underlying conceptual model -- or meta-model -- of the Riskit Analysis Graph components is presented in Figure 3. This meta-model represents the underlying, conceptual elements and their relationships. Each rectangle in the graph represents a risk element and each arrow describes the possible relationship between risk elements. The Riskit analysis graphs can be drawn with a diagram editor tools and there exist a template with the Riskit symbols available for the VISIO tool [26]. An example Riskit analysis graph is presented in Figure 4.

The Riskit analysis graph allows visual yet more formal documentation of risks, resulting in better communications and deeper, qualitative understanding of them.

3.4 Quantification of Risks

Most risk management approaches rely on risk estimation approaches that are either impractical or theoretically questionable. The expected value calculations [5] (i.e., risk = probability * loss) are often impractical because accurate estimates for probability and loss are seldom available and it is difficult to account for multiple goal effects and for the non-linear utility function.

Table-based risk ranking approaches [1,5,7,9,10] are often theoretically weak as they are based on performing multiplication on ordinal scale metrics – an operation that is mathematically meaningless and may result in incorrect rankings.

The Riskit largely avoids these problems by using ranking techniques that are matched to the type of information available. Expected value calculations are used when ratio or distance scale data is available. However, when only ordinal scale metrics are available for probability or loss, a specific *Riskit Pareto ranking technique* is used. This technique uses a two-dimensional space to position risk scenarios by their relative probability and utility loss. This technique can be explained by examples in Table 2: scenarios are positioned on the Riskit Pareto ranking table according to their rankings w.r.t. probability and utility loss. A scenario's Pareto efficiency over other scenarios can be easily assessed in the table: it is Pareto efficient if no other scenarios are in cell above it or left of it.

Using the Riskit Pareto ranking technique results in a partial ranking of risk scenarios, i.e., priorities for some scenarios can be defined but some scenarios' relative priority remains unknown. While the complete prioritization of scenarios would be desirable, the input data leading to the prioritization does not normally allow it.

In Table 2 scenario 1 is Pareto efficient over all other scenarios. The remaining scenarios can be only partially ranked based on the available information. The priority between scenarios 2 and 4 cannot be established but one can say that Scenarios 2 has higher priority than scenarios 3, 5, 6, and 7; and that scenario 4 has higher priority than scenarios 5, 6, and 7. The significance of these partial rankings is that they guide the focus of risk management to scenarios that have been reliably prioritized over other scenarios, given the information available. The risks should be considered for risk controlling action planning in their order of priority.

The value of the Riskit Pareto ranking technique is that it provides reliable and consistent ranking approach that only ranks risks as far as the input data allows.

3.5 Practical Application of Utility Theory

The importance of utility theory in decision making is well established in other disciplines [3,14,15], and while the concept has also been presented in software engineering risk management [4,9], it has not been made operational in any major risk management approach. Ignoring the impact of *utility loss* may seriously influence risk prioritization results. In most situations people and organizations have *non-linear* utility functions w.r.t. observable metric or attribute in question. In other words, the true benefit felt by a stakeholder does not have a linear function to, e.g., money, schedule or defect rate. Following example highlights the impact of non-linear utility function. Consider two bets:

- 50% chance of losing $200
- 1% chance of losing $10,000

The expected loss of these alternatives is the same ($100) but most people can clearly indicate which bet they would rather avoid. Such situations manifest the existence of non-linear utility function.

The Riskit method has incorporated the utility theory components into a straight-forward approach that can be used by practitioners without deeper knowledge of the utility theory. The risk scenario impacts are documented in effect sets in Riskit analysis graphs, as shown in Figure 4. The stakeholders are asked to compare the effect sets and indicate which ones cause the greatest utility loss to them, i.e., which effect sets would *hurt* them the most or cause them the most "*pain*". In most situations a pair-wise comparison of effect sets will yield accurate enough ordinal rankings of effects sets. However, if the situation is complex and more precise and reliable results are needed, multiple criteria decision making tools can be used to elicit utility loss preferences from stakeholders.

		Risk scenario probability				
		rank 1	*rank 2*	*rank 3*	…	*rank n*
Risk scenario Utility loss	*rank 1*	scenario 1	scenario 2		...	
	rank 2			scenario 3	...	
	rank 3	scenario 4	scenario 5	scenario 6	...	
	…	...	...	...	...	...
	rank m		scenario 7		...	

Table 2: Risk scenario ranking table using Pareto-efficient sets

4 Empirical Study Goals and Design

We have conducted several case studies for evaluating the Riskit method [11,21,22]. In this paper we present the findings from our empirical studies at Daimler-Benz AG and Nokia Telecommunications corporation. In the following we will present the case study design, organizations and their earlier risk management practices, as well as the findings from the case studies.

4.1 Case Study Objectives

The empirical studies were carried out in active, on-going, industrial projects. The primary motive for the organizations involved was to improve the risk management activities in the projects by introducing a well-defined risk management process. The research objectives in the projects were to

- Evaluate the feasibility and usefulness of the Riskit method in industrial projects, i.e., characterize its benefits and disadvantages and use this information for improving the method.
- Improve our understanding of the issues involved in introducing and improving risk management methods into software development programs, i.e.:
  - how well should the risk management infrastructure be defined,
  - how should the method be supported, and
  - how detailed risk analysis is feasible and necessary?

4.2 Instrumentation

Five forms of data collection were used in the case studies. First, the Riskit method itself produced extensive documentation about the risks and the risk management process that was followed.

Second, the risk management facilitators acted as observers in the risk management sessions and used this information as part of the analysis, taking notes and raising their observations in analysis sessions. This information was used to provide depth and context in the analysis of data, as well as to prompt observations in the sessions.

Third, a series of semi-structured interviews were performed to elicit participant feedback on the risk management process. The interview template contained 83 open questions and it was used to structure the interview session and to provide consistent coverage in interviews. In practice, interview sessions followed the interview template outline (Appendix A), but additional information was often volunteered in various points in the interview.

Fourth, Daimler-Benz had written a lessons learned report after the first risk management cycles in their projects, independently of the interview sessions held later. This report and its findings were included in the analysis.

Finally, in the Nokia case study we also used video recordings in the most critical sessions. This was done to avoid the potential observation bias by the method developer and to make sure that all relevant data was recorded. These recordings were analyzed to identify problems in the communications and to provide more information on the notes taken during the meetings. Video conferences were regularly used in this organization and some the risk management sessions did, in fact, take place between two continents.

	Daimler-Benz	Nokia
Frequency	Risks listed weekly in every subproject	Risks were listed in monthly
Formality	Reporting at project meetings within status reports	Monthly reporting of top 5 risks required
Method and tools	Documentation only for project tracking	Risks listed in order of importance
Identification techniques	By team members without any specific methods or techniques	By program and project managers without any specific methods.
Analysis techniques	No specific analysis techniques	Ranking based on numerical estimate of probability and qualitative estimate of impact on schedule and quality
Controlling and tracking techniques	Part of normal project management	Part of normal project management
Training	No specific training for risk management	No specific training for risk management

Table 3: Previous risk management in the two organizations

4.3 Case Study Designs

Both organizations had existing, relatively informal risk management practices in place prior to our case studies. Their earlier practices were analyzed through ethnographic techniques (spending time at the organization) and in the interviews. The highlights of these baselines are described in Table 3

The Riskit method was introduced to projects at an early phase of projects but not at their beginning. The Riskit method was used in slightly different way in the projects: at Daimler-Benz the method experts facilitated the sessions whereas at Nokia the project applied the method independently after an initial training and consulting period by the method developer.

4.4 Analysis Methods

Data from the case studies (participant observations, Riskit artifacts, interview notes and video recordings) were analyzed and relevant issues identified and highlighted. When an issue was highlighted, the experiences from the other case studies were compared to it and rationale and explanations were discussed.

4.5 Validity Threats

Case studies are prone to many limitations, compared to situations where large amounts of data can be collected and analyzed [25,27]. Studies in risk management, in particular, have even more serious constraints that limit the choice of experimental designs and available data points [21], as well as challenges in construct validity. In particular, low number of data points, their non-random selection, and variance in situational characteristics limit the external validity of the results obtained, i.e., their generalizability.

Our case studies tried to limit the internal validity threats associated with the descriptive part of our study by documenting and using raw data from the study and

recording the interview data as objectively as possible. We tried to provide a better basis for controlling external validity threats by explicitly documenting the situational characteristics of the cases, as well as replicating the study in two different organizations. However, the replication benefits were limited due to low process fidelity [13], as both organizations made modifications to original method.

Despite these limitations, we believe that our study produced data that has reasonably high internal validity and there are no major threats to the external validity of the results.

5 Case Study Data

The Daimler-Benz project was a business process re-engineering project that produced a diagnosis support system that will be distributed world-wide. The development involved both in-house development and the use of consultants, as well as in-house and commercial components. The project size was about 200 person years and duration three years. The Nokia case developed an embedded telecommunications product, involving well over 100 person years in less than two years. This project was in-house development involving advanced technologies and tools in a new organization, as well as including both software and hardware development.

5.1 Introducing Risk Management

The Riskit method was introduced and applied in slightly different ways in the two organizations, as shows. At Nokia the Riskit method was introduced to a product development program when the program was already running at full speed. Therefore, only minimal additional training was possible on risk management. The program defined a formal risk management process and included it in the program management procedures. However, the program manager reported that there were problems with process fidelity in practice (Appendix A, questions 14-16). The introduction of Riskit included making the Riskit documentation, drawing tools and templates available. General training on risk management and on the Riskit method were given to program management team in two single sessions. In addition, individual sessions were also given to key members of the management team.

	Daimler-Benz	Nokia
Scope of applying the method	Riskit process steps followed, Riskit analysis graphs used for most complex risks, different ranking technique used	Riskit process steps followed, Riskit analysis graphs used for key risks, Riskit ranking approach used
Way of applying the method	Sessions facilitated by a Riskit expert	Independent use (initial sessions facilitated by a Riskit author)
Training given on risk management	1 hour for project management, 1 hour in each subproject	Self study Two hour private session to project manager One-hour session to project management team
Number of risks identified and *documented*	30 at project level, up to 130 at subproject level	150
Number of risks controlled	10-20 on project level up to 20 (clustered) at subproject level	c. 70

Table 4: Characteristics of risk management processes

At Daimler-Benz the method was introduced and supported by two more experienced risk management experts that facilitated the risk management sessions in the project. They provided the training and defined project-specific conventions for risk management.

5.2 Risk Management Mandate

At Nokia the risk management mandate [19] was explicitly defined. The mandate provided better and unambiguous definition of the responsibilities and scope of risk management, compared to the situation before and thus contributed to more explicit risk management practices in the project (Appendix A, questions 19-24). The recognition of stakeholders clarified expectations and made the prioritization of goals easier, according to the program manager. However, the positions of some recognized stakeholders were not explicitly stated and this was a cause of concern to the project management (Appendix A, question 30).

At Daimler-Benz there was no formal risk management mandate definition, although some aspects of the mandate were defined (Appendix A, questions 20 to 25). In particular, the stakeholders were not defined. Project participants did not see any added value in spending time to re-analyze stakeholders. However, it was also observed that different project participants had different interpretations as to who are the relevant stakeholders and what their priority should be. We believe that part of the participants resistance to stakeholder analysis is caused by the smaller amount of training given at Daimler-Benz, as Table 4 indicates. Project participants may not have been aware of the rationale and benefits of stakeholder analysis.

These experiences indicate the following findings:

(f1) An explicit risk definition of risk management mandate seems to clarify the responsibilities and scope of risk management.

(f2) In order for stakeholder recognition to take place, participants need to be trained and motivated.

(f3) Without explicit stakeholder analysis participants are likely to have different interpretations of project's stakeholders.

(f4) Stakeholder information helps to understand and prioritize expectations and goals for the project.

5.3 Goal review

At Daimler-Benz the goal definition and goal review were based on project documentation, no specific goal analysis

sessions were held with project personnel. The goals were used to analyze risk effects, i.e., used in risk prioritization. As with the stakeholder analysis, project participants were not interested in discussing or re-analyzing goals, although different interpretations of goals were observed.

Some project participants expressed a concern that some goals are not well suited for open and explicit discussion ("*We will get problems [if] we are discussing [the] goals and write them down*"). We believe this is partially a cultural issue related to how openly goals are generally communicated, and partially a natural tendency of individuals to avoid over-commitment.

At Nokia there was an explicit goal review phase. This resulted raised several questions on the priority of the goals with respect to different stakeholders (Appendix A, question 27). This lead to re-definition and re-prioritization of some goals by the executive management. According to program management, the goal review raised the general awareness of program goals and their priority and helped understand the importance of some key constraints of the program, giving program management more flexibility and better focus (Appendix A, question 27). The Riskit approach seemed to help focus discussions, clarify concepts and points of view (Appendix A, question 30).

People participating in the goal review sessions initially had some motivation problems, they were not sure why a goal review is necessary in the project (Appendix A, question 28). This was probably due to the limited amount of training and motivation given to participants, since the goal review resulted in major changes in goals.

These experiences lead us to propose the following tentative conclusions:

(f5) An explicit goal review is provided useful input to project management in general.

(f6) Goal review requires motivation and training, as well as a right climate and attitude to result in open and complete analysis of goals.

5.4 Risk Identification

Different techniques were used for risk identification in both organizations: interviews, brainstorming and checklists. At Daimler-Benz the main technique was structured interviews. Riskit concepts were used to structure the interviews in which project members were asked about stakeholders, goals, risks and risk scenarios. Some subprojects wished to identify risks in workshops to optimize time for identification and analysis of risks. The free-format risk identification was supplemented by interviews. Checklists [8] were used to guide the workshops and a questionnaire was used to verify brainstorming results more analytically. The information gained in interviews seemed to be more detailed and of better quality than the results of workshops, perhaps due to more confidential nature of interviews and the possibility to focus on specific topics. The additional yield of using checklists in risk identification was small as the checklist did not match the domain of the project quite well.

According to Daimler-Benz experiences, the disadvantages of interviews are the large amount of information (risks have to be clustered) and the added time needed to achieve an agreement of the whole group.

In both organizations the raw risk data from initial identification sessions was clustered into groups based on some project-specific attributes. These clusters allowed better communication and filtering of risks for more detailed analysis. The clustering criteria varied between projects.

At Nokia, the risk identification had already been done previously in the program. A total of 60 risks had been identified and documented initially by individual sub-project managers, and during the program additional 90 risks were explicitly documented. The risk identification approach was an informal one and deviated from the Riskit process. The risk analysis in the program was done both at project level by project managers and at program level. The program level risk management was based on consolidating the project risks *and* evaluating risks from program perspective. The program manager expressed some concern about the coverage of risk identification approach that was used: some risks that occurred were not identified in the identification process (Appendix A, question 40)

Participants reported (Appendix A, questions 37 to 39) that separate risk identification sessions helped them think about risks proactively (instead of recognizing problems that are already present), consider long-term risks, and consider risk information from various sources.

Based on these experiences we suggest the following tentative conclusions:

(f7) It is difficult to ensure adequate coverage of risk identification without explicit risk identification techniques.

(f8) Checklists do not seem to yield many additional risks when used after free-format brainstorming sessions.

(f9) Project personnel are under constant time pressure and without enforcing explicit risk identification sessions they may not spend sufficient time in risk identification after the initial risk management cycle.

We also noted that generic risk management checklists may bias the risk identification, unless they represent the domain and project characteristics accurately.

5.5 Risk Analysis

At Nokia, the Riskit key concepts were used informally at subproject level but at the program level the main risks and risk scenarios were explicitly documented using the Riskit analysis graphs and ranked using the Pareto ranking table approach. The risk scenarios seemed to help analyze risks in more detail (Appendix A, question 51), but due to

limited training given, they remained distant and theoretical for many participants (Appendix A, question 50).

At Daimler-Benz the Riskit risk scenarios (documenting risk factors, risk events, and risk effects explicitly) seemed to result in deeper and unambiguous understanding of risks. However, our experience indicates that normally it is difficult to obtain the necessary detailed information for completing the risk scenarios (see Figure 4). Risk scenarios were sometimes left incomplete or they were too abstract to be of practical value. The Daimler-Benz experiences also indicated that developing risk scenarios requires more training and practice than was given in that case study.

Daimler-Benz used risk information sheets to document main information about risks in the process and these sheets become a central communication mechanism for the participants.

The risk scenarios seemed to improve transparency and understandability of risks, as well as increasing participants' confidence in the results.

Daimler-Benz did not use a Riskit based prioritization approach. Instead, they used two sets of risk ranking grids that were based on two-dimensional tables that ranked risk scenarios using probability, impact, urgency, and level of uncertainty. Risk scenarios were developed for risks that had high levels of uncertainty. Although there are some potential theoretical limitations with this approach, participants were satisfied with the approach and it was used consistently in the project.

Based on these experiences we suggest the following findings:

(f10) Riskit scenarios are perceived complex, at least when a minimal amount of training has been given to practitioners.

(f11) Riskit scenarios require training and facilitation before they can be used independently by project personnel.

(f12) Practitioners are satisfied using simple, straight-forward techniques in risk management, despite their potential, theoretical limitations.

5.6 General Observations

Overall the confidence of program participants on the risk management results increased with the Riskit-based risk management approach. There was a major shift in risk management thinking: earlier, risk identification was the main focus, now the risk controlling action received more focus and attention (Appendix A, question 81). This was not only supported by the risk management process but also by the templates that clearly guided the risk analysis towards risk controlling actions.

The systematic risk analysis also resulted in revised risk priorities. Based on the analysis of Nokia data, people's intuitive risk rankings were different from the rankings produced by the systematic risk ranking technique used in the Riskit process.

At Nokia, the use of Riskit seemed to increase the level of confidence in risk management results whereas at Daimler-Benz changes in confidence levels were not reported (Appendix A, questions 40, 58, 63, 68, and 80).

The Riskit method provided a conceptual framework that helped and structured discussions about risks (Appendix A, questions 30, 82)

The more detailed documentation of risks has allowed the organization to accumulate risk management experience and localized checklists based on actual risk history data are currently being developed.

Thus, additional findings can be summed up as follows:

(f13) The Riskit method seemed to encourage proactive risk management attitudes in the projects overall.

(f14) Intuitive risk rankings seem to differ from rankings derived using the Riskit method.

(f15) The use of systematic risk analysis methods seemed to increase participants' confidence levels in the results of risk analysis.

6 Conclusions

In this paper we have presented the Riskit method and reported experiences from its use in two organizations. In this conclusion section we will first review the case studies from the perspectives of the study goals we presented in section 4.1 and then present some generalized conclusions that, we believe, are likely to be applicable in other organizations as well.

The case studies supported the indications we have received earlier [20-22] that the Riskit method is a feasible approach for risk management in industrial context. It can be applied with reasonable initial training and it helps in performing risk management in software projects.

We have identified some findings from the case studies we carried out. We consider these findings tentative, as such a limited number of case studies makes it difficult to generalize the findings. These findings are presented in the following. We have made references to the findings listed earlier in the paper in parenthesis.

Risk management process must be supported and enforced (f1, f6, f9, f10, f11). Both case studies highlighted a common difficulty in risk management: it is difficult to make sure that the project organization consistently performs risk management. In particular, we observed a tendency to omit risk management towards the end of projects. We suggest that this trend can be avoided by improved training and support and by enforcing risk management consistently. Training for risk management should be given to all key project personnel so that they are fluent in risk management concepts and techniques. Our experience indicates that one or two hour training is not

adequate but half a day training with facilitated initial stage cycles may be sufficient.

Risk management should start before the project starts (f2, f4, f5, f13). Regardless of the risk management approach used, it is important to start the risk management activities as early as possible. For example, Daimler-Benz is currently initiating a new project and the scope of the project is being defined. In this project it is possible to address Riskit principles like stakeholder and goal orientation much better than in our earlier projects. These results were an important input for the clarification of what the project goals and who the stakeholders actually are.

Different risks require different documentation (f10). Some risks are clear and obvious when brief, informal description about them is given. Our case studies showed that it is not practical to document all risk scenarios with elaborate definitions and graphs. Sometimes it is not even possible to get all of the necessary information for Riskit Analysis Graphs. Riskit Analysis Graphs should be used when there is no consensus understanding on a risk or when there are significant uncertainties involved with risk. This will help clarify fuzzy areas and pinpoint the remaining uncertainties in a project.

Stakeholders and goals play a critical role in risk management (f3, f4, f5). The importance of stakeholders and their expectations was clearly demonstrated in the case studies: different participants had different understanding of stakeholders, their expectations and their priorities. Explicitly recognizing them will ensure that all relevant risk areas are better covered and the program can focus on essentials in their risk management.

A common risk management framework makes risk management efficient. Risk is a fuzzy concept term and it can mean different things to many people. The use of Riskit Analysis Graphs helped communications in some situations, but even when the risks were not documented graphically, the underlying concepts helped participants understand and communicate what aspect of risk was being discussed. This also allowed better delegation of risk management responsibilities and easier consolidation of such results. This

The Riskit process increased the confidence in risk analysis results (f14, f15). Based on our interviews, the explicit documentation of risks and the systematic risk ranking approach used provided participants full transparency to the risk analysis and its rationale, and they understood and trusted the analysis results better than they had done before.

Intuitive risk management produces different results compared to systematic, explicit risk management process (f14). There were many instances where the initial, intuitive perceptions of risks were significantly changed during the risk management process. We believe that the additional time spent on risk management as well as the methods used result in better understanding of risks and more appropriate risk controlling actions.

Risk identification requires special attention and a different mindset from other project and risk management activities (f7). Risk identification requires an open mind and ability to look beyond the obvious. While most of other management tasks in a project may rely on analytical thinking, risk identification requires ability to innovate. Therefore, risk identification sessions should be planned and supported to ensure adequate coverage of potential risks.

We plan to use the information gained in these case studies to develop the Riskit method further. We are currently working on defining more detailed application guidelines for the method, developing an approach for customizing checklists using the risk management information collected in the process, and providing better support for risk analysis through templates.

7 ACKNOWLEDGMENTS

We would like to thank participating organizations for their time and contributions in making this research possible. In particular, Pete Pihko at Nokia made his expertise and insights available for this research. We are also grateful for anonymous referees, whose comments encouraged us to provide more of the actual empirical data from the case studies to justify our findings.

8 REFERENCES

[1] Anonymous, Risk Assessment Techniques. In: *Defense Systems Management College Handbook*, Anonymous Defense Systems Management College, 1983. pp. iv-1--25, F-1--13.

[2] V.R. Basili, G. Caldiera, and H.D. Rombach. Goal Question Metric Paradigm. In: *Encyclopedia of Software Engineering*, ed. J.J. Marciniak. New York: John Wiley & Sons, 1994. pp. 528-532.

[3] P.L. Bernstein. *Against the Gods* , New York: John Wiley & Sons, 1996.

[4] B.W. Boehm. *Software Engineering Economics*, Englewood Cliffs, N.J.: Prentice Hall, 1981.

[5] B.W. Boehm. *Tutorial: Software Risk Management*, IEEE Computer Society Press, 1989.

[6] B.W. Boehm and Bose P., A Collaborative Spiral Software Process Model Based on Theory W 1994. Proceedings of the 3rd International Conference on the Software Process. IEEE Computer Society. Washington, DC.

[7] M.A. Caplan, Risk Management in Practice 1994. Proceedings of the Third SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.

[8] M.J. Carr, S.L. Konda, I.A. Monarch, F.C. Ulrich, and C.F. Walker. *Taxonomy-Based Risk Identification, SEI Technical Report SEI-93-TR-006*, Pittsburgh, PA: Software Engineering Institute, 1993.

[9] R.N. Charette. *Software Engineering Risk Analysis and Management*, New York: McGraw-Hill, 1989.

[10] A.J. Dorofee, J.A. Walker, C.J. Alberts, R.P. Higuera, T.J. Murray, and R.J. Williams. *Continuous Risk Management Guidebook*, Pittsburgh, PA: Software Engineering Institute, 1996.

[11] H. Englund, A Case Study to Explore Risk Management Methods 1997. Kunglika Tekniska Högskolan, Stockholm, Sweden. Masters thesis.

[12] R. Fairley, Risk Management for Software Projects *IEEE Software*, vol. 11, pp. 57-67, 1994.

[13] P.H. Feiler and W.S. Humphrey, Software Process Development and Enactment: Concepts and Definitions pp. 28-40, 1993. Proceedings of the 2nd International Conference on the Software Process, Berlin 1993. IEEE Computer Society Press. Los Alamitos, CA.

[14] S. French. *Decision Theory: An Introduction to the Mathematics of Rationality*, Chichester: Ellis Horwood, 1986.

[15] M. Friedman and L.J. Savage, The Utility Analysis of Choices Involving Risk *Journal of Political Economy*, vol. 56, pp. 279-304, 1948.

[16] A. Gemmer and P. Koch, Rockwell Case Studies in Risk Management 1994. Proceedings of the Third SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.

[17] J.C. Groth, Common-sense Risk Assessment *Management Decision*, vol. 30, pp. 10-16, 1992.

[18] IEEE, Managing Risk *IEEE Software*, vol. 14, no. 3, 1997.

[19] J. Kontio, The Riskit Method for Software Risk Management, version 1.00 CS-TR-3782 / UMIACS-TR-97-38, 1997. Computer Science Technical Reports. University of Maryland. College Park, MD.

[20] J. Kontio and V.R. Basili, Risk Knowledge Capture in the Riskit Method 1996. Proceedings of the 21st Software Engineering Workshop. NASA. Greenbelt, Maryland.

[21] J. Kontio and V.R. Basili, Empirical Evaluation of a Risk Management Method 1997. Proceedings of the SEI Conference on Risk Management. Software Engineering Institute. Pittsburgh, PA.

[22] J. Kontio, H. Englund, and V.R. Basili, Experiences from an Exploratory Case Study with a Software Risk Management Method CS-TR-3705, 1996. Computer Science Technical Reports. University of Maryland. College Park, Maryland.

[23] J.V. Michaels. *Technical Risk Management*, Upper Saddle River, NJ: Prentice Hall, 1996.

[24] G. Pandelios, Software Risk Evaluation and Team Risk Management 1996. Tutorial Presentations at the 1996 SEPG Conference. Software Engineering Institute. Pittsburgh, PA.

[25] J.L. Simon. *Basic Research Methods in Social Science*, New York: Random House, 1969. pp. -525

[26] Visio Corp., VISIO Technical, ver. 4.0, rel. 1995. Visio Corporation. IBM compatible PC. MS-Windows, Windows 95.

[27] R.K. Yin. *Case Study Research: Design and Methods*, Thousand Oaks, CA: SAGE Publications, 1994.

Appendix A: Interviewing Guidelines and Questions

Introduction

This appendix presents a structured interview template for the risk management experiences study done with Daimler-Benz and Nokia. This interview template is to be used to support consistent, semi-structured interviews for the cases that are analyzed in the study.

Study Goals

The study goal can be formulated as follows [2]:

Goal 1	*Analyze*	Risk management processes
	in order to	identify potential issues and observations
	with respect to	problems, benefits, disadvantages, improvement suggestions
	from perspective of	risk management process owners.
	In the context of	Daimler-Benz and Nokia

Interview Template

Interviewee Briefing

The interviewee should be briefed as follows:

> *This purpose of this interview is to collect your observations and experiences from the risk management activities in your project.*
>
> *It is of vital importance that you answer the questions as objectively and candidly as possible. We are using the interview information for research purposes only and, if you wish, we can guarantee total anonymity for your or your organization's participation in this study.*

Questions

Background Information

1 Interviewee's name:
2 Position at the organization:
3 Role in the project:
4 Open characterization of project planning and management experience of the interviewee:
5 Years of experience in project management:
6 Training received in project planning or estimation:
7 Were you involved in the definition of project goals, schedule and project contract?
8 Who else was involved in this process?
9 How important was your role in it?
10 Years of experience in risk management:
11 How much training have you received in risk management?

Interview Questions

The interview will be carried out by main steps of the Riskit process.

Risk Management Infrastructure

In your own words, characterize your project's risk management infrastructure along the following main attributes:

12 *Culture* – the level of awareness about risk management and attitude towards risks and risk management. The risk management culture can be characterized by question as is organization risk-averse or risk-taking, is the discussion about risks encouraged, is risk management recognized as a legitimate activity.
13 Policy – the stated management commitment to risk management and how it is enforced.
14 Methods: what methods and techniques are used and supported for risk management.
15 Tools – what tools and templates are used in risk management.
16 Skills and competence – what risk management skills and competencies exist, what training is available and given to personnel for risk management.
17 Support structure – what type of organizational support exists to help perform risk management in projects, how much resources are made available for this task.
18 Experience capture process – what mechanisms exist to capture, accumulate and analyze risk management experience.

Risk Management Mandate

19 Was risk management mandate defined (informally or formally)?

Characterize whether the following attributes of the risk management mandate were defined at the beginning of the project and how they were characterized:

20 Objectives:
21 Scope:
22 Risk management authority:
23 Accepted risks:
24 Risk management procedures:

25 Stakeholders:

Goal Review

26 How were goals defined?
27 What was the impact of having goals defined?
28 What problems occurred in this step?
29 What do you think are the main benefits of the approach used?
30 What technique was most useful technique in this step?
31 What impact did the goal definition have on the project, in your opinion?

Risk Identification

32 How were risks identified:
33 What techniques were used?
34 How much time was spent?
35 Who participated?
36 How many risks were identified?
37 What problems occurred in this step?
38 What do you think are the main benefits of the approaches used?
39 What technique was most useful technique in this step?
40 How much confidence did you have in having had adequate coverage of the risks?

Risk Analysis

Risks Item Clustering

41 How were risks clustered?
42 How many groups?
43 What criteria was used for clustering?
44 What problems occurred in this step?
45 What do you think are the main benefits of the approach used?
46 What technique was most useful technique in this step?

Risk Scenario Development

47 Were risk scenarios defined?
48 How many scenarios were defined?
49 How complex were scenarios?
50 What problems occurred in this step?
51 What do you think are the main benefits of the approach used?
52 What technique was most useful technique in this step?
53 What impact did the scenarios have on the project, in your opinion?

Risk Prioritization

54 How were risks prioritized?
55 What problems occurred in this step?
56 What do you think are the main benefits of the approach used?
57 What technique was most useful technique in this step?
58 How much confidence did you have in having prioritized the risks correctly?

Risk Control Planning

Defining Risk Controlling Action

59 How were risk controlling actions defined?
60 What problems occurred in this step?
61 What do you think are the main benefits of the approach used?
62 What technique was most useful technique in this step?
63 How much confidence did you have in having had enough potential risk controlling actions considered?

Selecting Risk Controlling Action

64 How were risk controlling actions prioritized and selected?
65 What problems occurred in this step?
66 What do you think are the main benefits of the approach used?
67 What technique was most useful technique in this step?
68 How much confidence did you have in having selected the right risk controlling actions?

Risk Control

69 How were risk controlling actions implemented?
70 Was their implementation tracked?
71 What problems occurred in this step?
72 What do you think are the main benefits of the approach used, if any?
73 What technique was most useful technique in this step, if any?

Risk Monitoring

74 How was risk situation monitored?
75 Frequency of monitoring?
76 Responsibility?
77 What problems occurred in this step?
78 What do you think are the main benefits of the approach used?
79 What technique was most useful technique in this step?
80 How much confidence did you have in having performed the risk monitoring activity adequately?

Concluding questions

81 Overall, what was the impact of risk management in the project?
82 What are the most critical problem areas in risk management?
83 What techniques would require more clarification or help in the methods used?