An Industrial Case Study of Implementing Software Risk Management

Bernd Freimut, Susanne Hartkopf, Peter Kaiser
Fraunhofer IESE
Sauerwiesen 6
D-67661 Kaiserslautern
+49 (0) 6301 707 263
{freimut,hartkopf,kaiser}@iese.fhg.de

Jyrki Kontio
Helsinki University of Technology
P.O. Box 1100
FIN-02015 HUT
+358-9-451-4852
jyrki.kontio@cs.hut.fi

Werner Kobitzsch
Tenovis GmbH&Co KG
Kleyerstraße 94
D-60326 Frankfurt am Main
+49 (0) 69 7505 6010
werner.kobitzsch@tenovis.com

ABSTRACT

Explicit risk management is gaining ground in industrial software development projects. However, there are few empirical studies that investigate the transfer of explicit risk management into industry, the adequacy of the risk management approaches to the constraints of industrial contexts, or their cost-benefit. This paper presents results from a case study that introduced a systematic risk management method, namely the Riskit method, into a large German telecommunication company. The objective of the case study was (1) to analyze the *usefulness and adequacy* of the *Riskit method* and (2) to analyze the *cost-benefit* of the *Riskit method* in this industrial context. The results of (1) also aimed at improvement and customization of the Riskit method. Moreover, we compare our findings with results of previous case studies to obtain more generalized conclusions on the Riskit method. Our results showed that the Riskit method is practical, adds value to the project, and that its key concepts are understood and usable in practice. Additionally, many lessons learned are reported that are useful for the general audience who wants to transfer risk management into new projects.

Keywords

Risk Management, Case Study, Lessons Learned, Riskit Method

1. INTRODUCTION

Since the introduction of risk management into the mainstream of software engineering [7][12], the software industry has gradually become more active in using explicit risk management [13][22]. Also, the increased requirements for risk management by many assessment standards have increased corporate interest in risk management.

Risk management practices have become much more operational and practical, as many guidelines, textbooks [14][20], and consultants help organizations improve their risk management practices.

Yet, while industry is clearly using risk management techniques more actively, there are only few reports available on experiences of introducing risk management into an organization. The reports that are available have been conducted as informal case studies without sufficient attempt to scientific rigor or empirical research methods [4][9][11][17][29]. However, systematic empirical investigations are necessary to learn more about the transfer and application of risk management methods.

To contribute such a systematic empirical investigation, this paper presents a carefully designed case study on the implementation of a specific risk management method, namely the Riskit method, into the telecommunication company Tenovis.

The paper builds on a series of three case studies related to the Riskit method [18][24][27]. The value of replicated case studies of the same method in varying contexts allows us to generalize our findings with respect to Riskit in particular and risk management in general. Additionally, replication in different contexts allows us to identify important context factors affecting the success of the transfer and implementation of risk management.

The objectives of the case study presented in this paper were twofold. The first objective was to characterize the *usefulness and adequacy* of the *Riskit risk management process* from the viewpoint of the *risk management participants*. This objective aimed at identifying effective ways of introducing risk management at the company in question and in general, and of providing feedback for improving the Riskit method.

The second objective was to characterize the *cost-benefit* of the *Riskit risk management process* in the context of *Tenovis*. This objective was to investigate the economic impact of the Riskit method.

The remainder of the paper is structured as follows. Section 2 describes the transferred risk management method. Sections 3 and 4 describe the project selected for this case study and the transfer of risk management into the project. Section 5 describes the design

of our case study. The results of this case study are presented and compared with the results of previous case studies in Section 6. Based on these results, we infer in Section 7 lessons learned that are relevant for the general community. Section 8 concludes the paper with a summary.

2. THE RISK MANAGEMENT METHOD

The risk management method transferred in this case study is called Riskit. Riskit is a comprehensive risk management method that is based on sound theoretical principles, yet it has been designed to have sufficiently low overhead and complexity so that it can be used in real, time-constrained projects. Because of its more solid theoretical foundations, it avoids many of the limitations and problems that are common to many other risk management approaches in software engineering, such as use of biased ranking tables and expected value calculations. As Riskit has been extensively presented in other publications [23][24][25][26][27], we present here only the principles of the method and the features that distinguish it from other risk management approaches.

Riskit contains a fully defined process, whose overview is presented in Figure 1 as a dataflow diagram. The full definition of the Riskit process is available as a separate report[25].

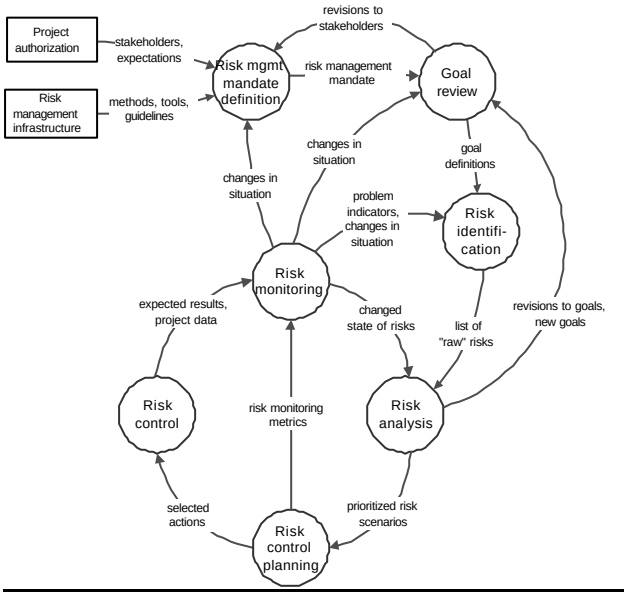


Figure 1: Overview on Riskit process

The Riskit process includes a specific step for analyzing stakeholder interests and how they link to risks. These links are visualized in Figure 2: when risks are defined, their impact on the 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 his perspective.

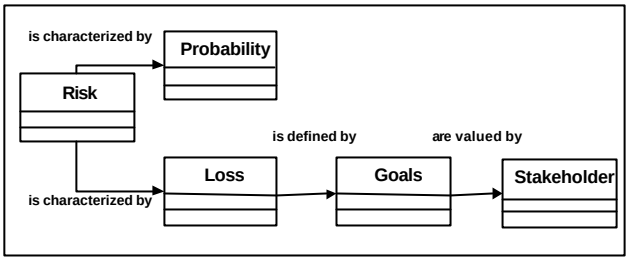


Figure 2: Definition of Risk within Riskit

In order to describe risks during Risk analysis, the Riskit method supports unambiguous definition of risks using the *Riskit analysis graph* (also called risk scenario) as a visual formalism. The Riskit analysis graph can be seen both as a conceptual template for defining risks as well as a well-defined graphical modeling formalism. An example Riskit analysis graph is presented in Figure 3. The Riskit analysis graph allows visual yet more formal documentation of risks, resulting in better communications and a comprehensive understanding of the risks' context.

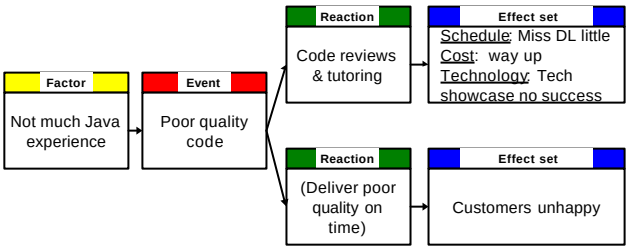


Figure 3: Example of the Riskit analysis graph (risk scenarios)

In order to prioritize risks during Risk analysis, the most important risks have to be selected based on their probability and loss. To perform this prioritization, most risk management approaches rely on risk estimation approaches that are either impractical or theoretically questionable. For example, the expected value calculations (i.e., risk = probability * loss) [7] are often impractical because accurate estimates of probability and loss are seldom available and it is difficult to account for multiple goal effects and for a non-linear utility function.

Riskit largely avoids these problems by using ranking techniques that are appropriate for the type of information available. When ratio or distance scale data are available for probability and loss, expected utility loss calculations are used. However, often only ordinal scale metrics are available for probability or utility loss. For example, the risk scenarios might be ranked in terms of probability and utility loss each as shown in Figure 4.

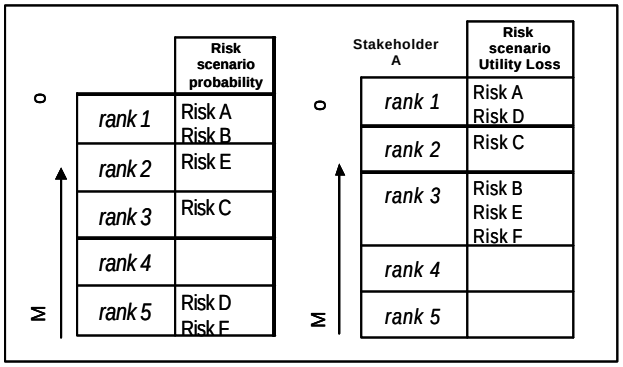


Figure 4: Ordinal Metrics for Probability and Loss

To select in this case the most important risks based on the combination of probability and utility 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 as shown in Figure 5. Using this technique, the evaluation of the risks is then based on utility theory [3][16].

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

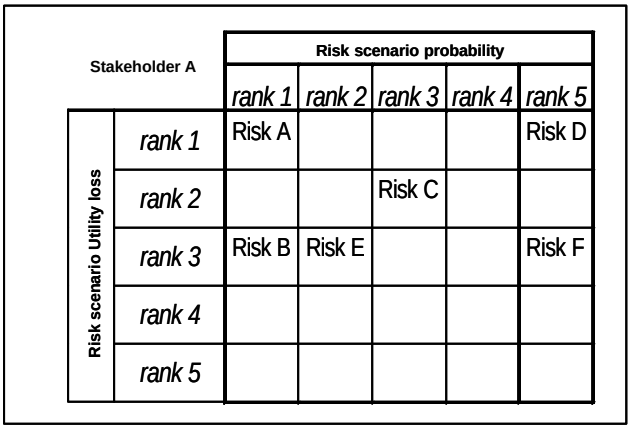


Figure 5: Example of Riskit Pareto Table

3. CASE STUDY CONTEXT

Tenovis is one of Germany's largest companies in the telecommunication market. It is a successor of Bosch Telecom and has about 8500 employees. Tenovis works in a wide range of telecommunication areas such as private branch exchanges (PBX), call centers, and IP-based telephony.

The project considered in this case study aimed to provide a unified, integrated tool to support service personnel in their task of administrating all of Tenovis' existing PBX platforms. Thus, this project was called Tool Harmonization Project. Starting at the end of 1999, the project's duration was planned to be approximately one year.

In this project new and challenging technologies were to be applied. Web technology was to be used in a client-server application context. Additionally, object-oriented technology was selected for design and implementation. On the one hand, the new technologies added complexity to the project, on the other hand, they were expected to increase the project's productivity. Besides the new technologies, a new development process and a new project organization were introduced, which involved teams from three different locations and time zones (India, France, and Germany).

In the early stages of the project, risk management was performed in an informal way. However, this intuitive risk management was considered to be longer appropriate for a company in the telecommunication market. This market is characterized by high competition, strong demand for innovative technologies, and a very short innovation cycle. These factors usually impose risks to telecommunication projects. The introduction of new technologies and processes imposed additional risks. Hence this project was seen as particularly risky compared to other projects at Tenovis. This situation made the case for the introduction of explicit, systematic, and experience-based risk management into this project.

4. TRANSFER OF RISK MANAGEMENT

The transfer of risk management to the Tenovis context was entrusted to Fraunhofer IESE, which served as methodology provider.

The Riskit method (see Section 2) method was one part of the overall risk management concept proposed to Tenovis. Additionally, this concept included methods to support risk management by data and to re-use risk experience in future projects. Risk management by data uses specific data from a measurement program to provide status information on a project. Risk management by experience enables learning from other projects by means of an experience factory [2]. This paper, however, deals only with the application of Riskit.

In the beginning, a kick-off workshop took place. The participants in this workshop were the department head, who sponsored the implementation of risk management, and the project management team. In the workshop, a tutorial on Riskit was given. Additionally, the activities of mandate and goal definition, risk identification, risk analysis, and risk control planning (cf. Figure 1) were briefly performed for the concrete project. A similar workshop was later performed for senior developers. We also defined specific templates for documenting risk information during the project (see Figure 7).

For subsequent risk management activities, which were held in separate meetings in addition to the regular project meetings, a risk management team was established. This team consisted of the department head and two members of the project management team. The latter ones changed over time.

The risk management team was supported by the personnel from Fraunhofer IESE, who had the role of facilitators in the risk management meetings. In this role they prepared the meetings by,

for example, selecting and preparing the risk management techniques to be applied, providing the necessary documents, and sending invitations. During the meetings they moderated the discussions and took care of the correct application of the risk management techniques. In addition, they were responsible for the documentation of the meeting results.

In the course of the project, the introduction of risk management was negatively affected by several circumstances. First, the project members regarded risk management as "yet another new method" besides the new process and technologies, resulting in low motivation for it. Second, the project manager, who played a very prominent role in risk management, changed. Third, the company was sold, resulting in a major restructuring, which made it difficult for some time to work regularly on risk management.

5. CASE STUDY DESIGN

The empirical study reported in this paper is a carefully designed case study with predefined objectives and some level of control with respect to the overall arrangements of the study. The authors were observing the study while facilitating it.

The design of the case study started at the beginning of the technology transfer. We first identified the research goals shown below in the form of a GQM-goal template [8][33]:

G1: Characterize the *usefulness and adequacy* of the *Riskit risk management process* from the viewpoint of the *risk management participants* in the context of *Tenovis*.

To us usefulness and adequacy mean the advantages and drawbacks of risk management with respect to (1) the Riskit features, (i.e., the techniques used within Riskit), (2) performing explicit risk management in general, (i.e., Riskit-independent issues), and (3) the transfer of the risk management process and methods into the project.

G2: Characterize the *cost-benefit* of the *Riskit risk management process* from the viewpoint of the *department head* and the *project manager* in the context of *Tenovis*.

This goal aimed at assessing the economical impact of the transferred risk management technology.

Using the Goal-Question-Metric Paradigm [8][33], we refined these two goals in questions characterizing the quality aspects usefulness, adequacy, and cost-benefit. Subsequently, we refined these questions into metrics defining the data to be collected to answer the questions and evaluate the research goals. The identified metrics were of two types: quantitative metrics and qualitative metrics.

The quantitative metrics included information like the effort spent on risk management, the number of risks and risk types over time, the number of controlling actions and their effectiveness over time. We collected data for these metrics regularly during the performance of risk management. Most of the data were collected as part of the risk management documentation.

The qualitative metrics included aspects like the benefit of risk management as perceived by the participants and the advantages and drawbacks of the employed Riskit process and its techniques as seen by the participants. To collect the data for these metrics, we prepared a questionnaire containing 33 questions and an associated interview procedure (cf. Figure 6) for a structured interview. Using these materials, we interviewed all five members of the Tenovis risk management team at the end of the project, with each interview lasting about one hour. The interviews were held with one interviewer and one scribe who recorded the interviewees' answers. The recorded answers were entered into a database for better analysis. Each interviewee was sent a report with his entered answers for review.

Questions wrt. Risk Management Process

First, open discussion on steps, their objectives and main benefits.

1. Consider the risk management process. Please explain from your point of view the risk management process. For each step, we would like to know from your point of view the **objective** of the step, and the **main benefit** of the step.
   F after initial open question show figure to ask specifically for remaining ones

The next set of questions concerns the usefulness of the applied techniques and the presentation of the techniques.

19. Considering the techniques applied in the process (see figure), which **techniques** were particular **useful** and which techniques should be thought over (and why?)?
    F (esp.: risk identification: difference between brainstorming, checklists)
20. F Was the development of risks into **RiskIt-Scenarios helpful** for an understanding of the risk?
21. F What do you think about the **documentation** of the risks as **RiskIt Scenarios**? (was appropriate, too laborious)?
22. F Did you have **appropriate information to perform the comparison** to identify the worse or more likely scenario? (if not: what was missing or difficult?)
23. F Was the selection of TOP10 risks using the **Pareto table** comprehensible or were there problems? (which problems?)
24. F Were the **monitoring questions** useful for determining risk and project status?
25. F Was the **information on the risk sheet** appropriate for risk monitoring?
26. F In general, was the **level of detail** in the risk scenario forms too much, enough, not enough?
27. Where there any **steps** in the RM process that, in your opinion, have **improvement potential**. If yes, in which step and what can be done better?

Figure 6: Excerpt of interview procedure

The interview results were combined and analyzed in order to answer the research goals and identify the strengths and weaknesses of the employed approach. In addition to the interview results, we also used the observations we made as facilitators of the risk management meetings. These observations were recorded after each meeting in a logbook and mainly referred to practices that worked well or were unpractical.

Based on the interview results and the recorded observations we devised a set of improvement suggestions to improve the risk management process and to better tailor it to the environment.

To verify our conclusions and suggested process improvement proposals, a feedback session with the members of the risk management team (i.e., the interviewees) was performed. The improved risk management process will form the basis for future risk management activities at Tenovis.

Empirical studies in general and case studies in particular are prone to biases and validity threats that make it difficult to control the quality of the study and to generalize its results [32][34]. In the following we discuss selected, relevant validity threats and

describe the steps taken to reduce them or their impact on our study.

The *reliability* of our data collection (i.e., its consistency and repeatability) was improved by documenting the interview questions and interview procedure in detail and applying them consistently.

The two main threats to internal validity in the study were experimenter expectation bias and maturation [35]. The *experimenter expectation bias* could occur due to the technology providers' expectations or desire to see positive results in a study. This bias was reduced by carefully discussing and evaluating the facilitator observations and findings and emphasizing the Tenovis participant feedback on them. Also, we kept logbooks after each meeting to record our observations in their original form, which helped us to remember the precise observations and their contexts even after some time.

The *maturation effect* threatens the conclusions of a study when subjects react differently as time passes. In our case this could have been possible as the participants were just going up their learning curve on risk management and thus became more fluent in its activities over time. However, the interviews took place at the end of the project in a short period of time when the participants were quite mature in their risk management practices. Therefore, we believe that the maturation effect did not significantly affect our study.

The *representativeness* of the project and its participants relates to how well we can generalize the results, i.e., to external validity. The project itself was more risky and had perhaps higher expectation levels than normal projects in the company. We believe that this had two impacts: On the one hand, this may have biased the participants to recognize the need for risk management more clearly, resulting in a generally positive attitude towards risk management. On the other hand, the pressures of aggressive project goals may have also reduced the time available for risk management activities by simultaneously increasing the expectations from risk management results. This could have resulted in a more negative attitude towards the impact of risk management on the project. Regarding the representativeness of the project participants, we have no specific reason or information to believe that the participants would be different from those of other projects.

6. CASE STUDY RESULTS

6.1 Results for Riskit's Usefulness

In this section we report the findings of our observations and the interviews. Section 6.1.1 describes our findings related to the Riskit method itself, Section 6.1.2 describes our findings related to the performance of the risk management in the Tenovis project, and Section 6.1.3 describes our findings related to the transfer of risk management into the context of Tenovis.

6.1.1 Usefulness/Adequacy of the Riskit Process

One crucial element in the interviews was the question: *For each activity in the Riskit process, what are the advantages and problems perceived by the participants?* In the following, we report the most important findings related to the individual activities and techniques in the Riskit process.

Process definition: One feature of Riskit is the full operational definition of its process. This explicit process was perceived as systematic and very helpful. Unlike "intuitive" risk management, where risks are unsystematically identified at the beginning and not appropriately tracked, the process triggers all necessary activities. One positive side effect of the explicit process is also that the importance of risk management is emphasized as people dedicate their time to work specifically on risk management activities.

Risk Identification: To identify risks, the Riskit process provides two techniques, which compensate each other's biases. The two techniques are brainstorming and a risk checklist. In this case, we used an excerpt of the SEI checklists for risks [10].

The combination of these techniques was appreciated as being systematic and comprehensive. Retrospectively, the participants noted that most of the project's risks were identified during risk identification. Additionally, the composition of the risk management team of people from different roles (i.e., people with a different view on the project) was beneficial, as the different views on potential risks could be exchanged and combined. Consequently, almost all participants learned about risks that were new to them.

Risk Analysis: As shown in Figure 3, Riskit uses Analysis Graphs to describe and discuss risks.

These Analysis Graphs were rated as very helpful in understanding the risk, its context, and its consequences. One benefit of these graphs was clearly the visual representation, which made the risks more explicit and facilitated discussions about them.

Although the development of these graphs was time consuming (discussion of a risk event and development of the corresponding scenario took about 17 min on average), participants regarded this time as well-invested due to the increased understanding of the risks.

Another feature of the Riskit method is the Pareto ranking technique to rank risks and select the most important ones.

This Pareto ranking technique was perceived as beneficial and practical as people could easily compare the risks in terms of probability and utility loss. Especially for the latter it was appreciated that no precise, quantitative estimate of the loss had to be given but measurement was performed through ranking the risks (i.e., for two risks it had only to be determined, which risk had the larger loss). The selection of the most important risks based on the combination of probability and loss was performed

by means of a Pareto-table [25]. This selection was regarded as comprehensible and thus, participants appreciated this technique.

Documentation: The documentation of the process activities is performed by means of a set of forms. These forms serve the communication between different activities of the process as well as between different meetings. The most central form is the Risk Scenario Form (cf. Figure 7).

This form contains a description of the risk in both textual and graphical form, the risk's ranking in terms of probability and utility loss, potential and implemented controlling actions, as well as a history of the risk and its controlling actions. Thus, it contains complete information both for operational purposes (i.e., monitoring of controlling actions) and documentation purposes (which are supposed to enable learning from risks for future projects).

Based on the interviews, three disadvantages of the forms were observed. First, the forms contain too much information for daily work, especially for risk monitoring. During risk monitoring, participants were only interested in the graphical description of the risk and the list of controlling actions. Consequently, the remaining information was seen as superfluous for this activity.

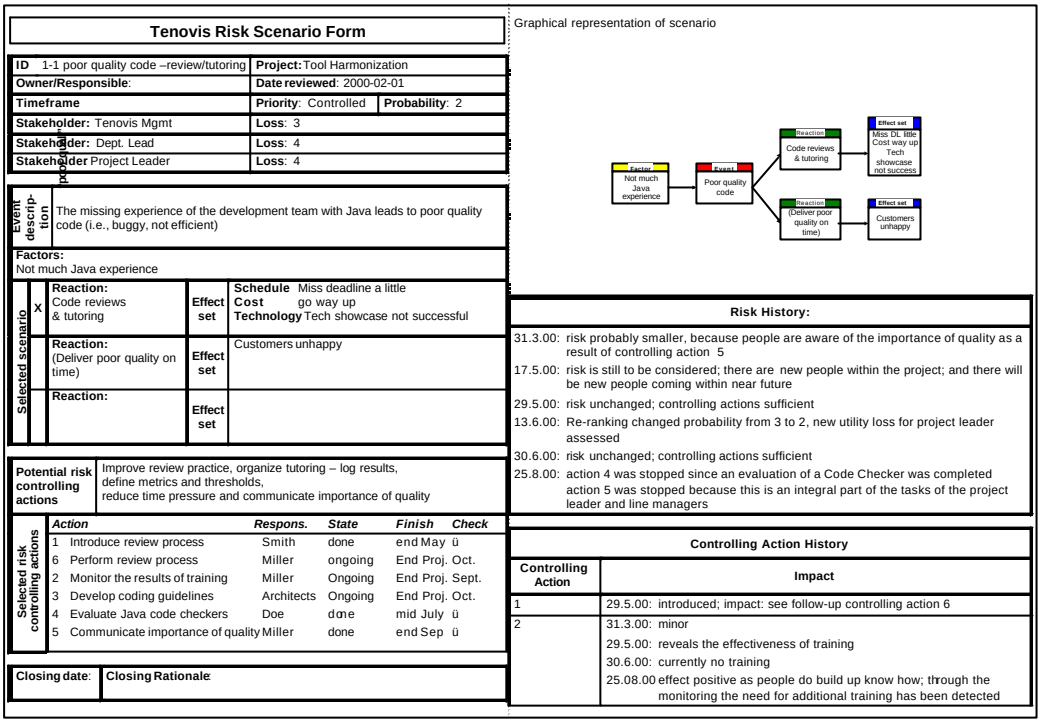
Second, the textual description of the risks was kept very short and thus mainly consisted of keywords. This amount of detail was sufficient as long as the participants remained the same. However, in the course of the project, new members joined the risk management team. For them it was difficult to acquire the necessary understanding of the risks due to their short description. The lack of clear descriptions has the additional disadvantage of complicating the re-use of risk experience in future projects.

Third, the effort for maintaining the documentation was considered too high (cf. Figure 8). After a risk monitoring meeting, which was to be performed bi-weekly, the facilitator team spent about two hours on updating the statuses of the controlling actions as well as the risk and controlling action histories. Responsible for the high effort was mainly the fact that the update was performed manually in the entire documentation, which was written in MS-Word with a complex link structure.

This drawback of the process in terms of documentation overhead can be easily overcome by an appropriate tool support for the documentation, such as a simple database solution. This solution also enables project managers to have fast access to risk information.

Summarizing our findings with respect to the Riskit method, we can conclude:

- The explicit process of the Riskit method was regarded as systematic and practical.
- The techniques used within the Riskit method were regarded as practical and understandable. The distinguishing features of Riskit, especially, were regarded as particularly valuable.



Tenovis Risk Scenario Form

Graphical representation of scenario

ID 1-1 poor quality code –review/tutoring	**Project:** Tool Harmonization	
Owner/Responsible:	**Date reviewed**: 2000-02-01	
Timeframe	**Priority**: Controlled	**Probability**: 2
Stakeholder: Tenovis Mgmt	**Loss**: 3	
Stakeholder: Dept. Lead	**Loss**: 4	
Stakeholder Project Leader	**Loss**: 4	

Event description (product risk): The missing experience of the development team with Java leads to poor quality code (i.e., buggy, not efficient)

Factors: Not much Java experience

Selected scenario

	Reaction	Effect set
X	Code reviews & tutoring	**Schedule** Miss deadline a little **Cost** go way up **Technology** Tech showcase not successful
	(Deliver poor quality on time)	Customers unhappy

Potential risk controlling actions: Improve review practice, organize tutoring – log results, define metrics and thresholds, reduce time pressure and communicate importance of quality

Selected risk controlling actions

	Action	*Respons.*	*State*	*Finish*	*Check*
1	Introduce review process	Smith	done	end May	ü
6	Perform review process	Miller	ongoing	End Proj.	Oct.
2	Monitor the results of training	Miller	Ongoing	End Proj.	Sept.
3	Develop coding guidelines	Architects	Ongoing	End Proj.	Oct.
4	Evaluate Java code checkers	Doe	done	mid July	ü
5	Communicate importance of quality	Miller	done	end Sep	ü

Closing date: **Closing Rationale**:

Risk History:

31.3.00:	risk probably smaller, because people are aware of the importance of quality as a result of controlling action 5
17.5.00:	risk is still to be considered; there are new people within the project; and there will be new people coming within near future
29.5.00:	risk unchanged; controlling actions sufficient
13.6.00:	Re-ranking changed probability from 3 to 2, new utility loss for project leader assessed
30.6.00:	risk unchanged; controlling actions sufficient
25.8.00:	action 4 was stopped since an evaluation of a Code Checker was completed action 5 was stopped because this is an integral part of the tasks of the project leader and line managers

Controlling Action History

Controlling Action	Impact
1	29.5.00: introduced; impact: see follow-up controlling action 6
2	31.3.00: minor 29.5.00: reveals the effectiveness of training 30.6.00: currently no training 25.08.00 effect positive as people do build up know how; through the monitoring the need for additional training has been detected

Figure 7: Risk Scenario Form for one risk event

6.1.2 Instantiation of Risk Management at Tenovis

The crucial question *For each activity in the Riskit process, what are the advantages and problems perceived by the participants?*[1] also provided observations that did not directly refer to the Riskit method itself but more to the way risk management was instantiated at Tenovis. Thus, these observations are of a more general nature.

Integration with project management and project work: The activities of the Riskit process were performed in dedicated meetings with the members of the risk management team. This was also true for the more frequent risk monitoring meetings. This separation from the project meetings was retrospectively seen as a drawback, since the project members (especially sub-project managers but also developers) were not included in the risk management activities.

To overcome this problem in the future, a stronger linkage between project work and risk management is intended.

Risk Identification: In this project, risk identification was performed intensively at the beginning. Yet, although during risk monitoring, several new risks were identified spontaneously, no risk identification meeting was performed in the subsequent course of the project. This fact was seen as a drawback as risks that were unknown at the beginning of the project were not systematically included in risk management.

Therefore, in the future, risk identification meetings will be scheduled automatically at pre-defined milestones.

Risk Monitoring: Risk Monitoring is one of the crucial activities in the risk management process. The importance stems from the fact that this activity has to be performed regularly within the regular project work (e.g., weekly or bi-weekly) and therefore should also be as short and concise as possible.

Two drawbacks were observed with our approach. First, although bi-weekly risk monitoring meetings were intended, it turned out that the intervals between the risk management meetings were longer due to non-availability of the facilitators and participants. These long intervals were perceived as too long, as it was not possible to react quickly enough to changes in the risk and controlling action statuses. Moreover, due to the long intervals, it was difficult for participants to remember the context of the risks and their controlling actions.

Second, it is the task of risk monitoring to assess the status and effectiveness of the controlling actions. In the project, this was done by asking about the status of the controlling action, its impact on the risk (where usually a rating of {high, medium, low} or a short sentence was given), and whether the combination of controlling actions effectively controls the risk.

Retrospectively, the participants thought that the controlling actions were not performed as planned and therefore were not as effective as they could have been. This could have been prevented

[1] This high-level question was refined in the actual questionnaire and related to all activities and techniques in the Riskit process.

by more strongly questioning the controlling action. Thus, in the future, the actual implementation of the controlling action (what?) and its impact on the risk (how good?) has to be more strongly questioned.

Summarizing our findings related to the instantiation of risk management, we can conclude:

- Risk management should be closely integrated with project management and daily project work to foster the synergy between these activities.
- Risk identification should be scheduled automatically at predefined milestones (and, additionally, whenever it is seen as necessary).
- Risk monitoring should be performed regularly with short intervals between two meetings.
- Risk monitoring has to sufficiently question the implementation of controlling actions and their impact on risks.

6.1.3 Adequacy of the Transfer

The third set of results refers to the findings related to the transfer of risk management into the context of Tenovis. To assess the adequacy of the transfer, the questionnaire contained the questions like *How did you perceive the work split between Tenovis and IESE?* and *From your point of view, how strong was the commitment for risk management from the {architects[2], management, yourself}?*

Training: The training given to participants was seen as essential as it provided the necessary background for risk management and its techniques in general as well as for Riskit in particular.

In the future, however, not only the project and department management should take part in the training but also the developers. The purpose is, on the one hand, to enable developers to perform risk management activities (as risk management is to be more included in the project work). On the other hand, the training can also raise the awareness of risk management and risks.

Process Ownership: As described in Section 4, the technology was transferred by the personnel from IESE, who performed the entire facilitation in the meetings and maintained the documentation. The facilitators also triggered the risk management meetings. Initially, it was planned to give this responsibility to the Tenovis personnel in the course of the project, but due to time restrictions this did not happen as planned.

Thus, process ownership remained with the facilitators and not with the project management team or even the Tenovis company. Consequently, participants often had the impression that risk management was not part of their daily project work but rather an additional activity for an external party.

To improve this in the future, the process ownership for risk management has to rest with the project manager, who has to take care of the execution of the process, invite the participants to the risk management meetings, and ensure implementation of the controlling actions.

Thus, the role of the technology provider IESE should be to facilitate the first few sessions, take part in the following sessions as observers, and finally leave the entire facilitation to the Tenovis risk management personnel.

Commitment of project manager: A third important observation concerns the involvement of the project manager in the technology transfer. In risk management, the project manager is the crucial person as s/he is the person making decisions and being responsible for the activities in the project. This also includes activities that arise from controlling actions, and motivating the development team. Moreover, risk management is part of his/her project management task.

The actual approach of our transfer was prone to give the project manager the impression that an external party (i.e., the facilitators) intervened in his tasks and authorities as project manager. Therefore, in addition to the changed technology transfer approach (see above), the commitment of the project leader has to be ensured from the beginning and the transfer approach must be coordinated with the project manager.

Summarizing our findings related to the transfer of risk management, we can conclude:

- Training of the employed risk management process is important to train the participants and raise awareness for risk management and risks.
- Process Ownership for risk management has to rest with the project manager.
- Commitment of the project manager is of utmost importance and has to be ensured from the beginning.

6.2 Results for the Cost-Benefit of Riskit

An important criterion for introducing a new technology is its cost-benefit relationship. For risk management, however, this relationship is hard to express quantitatively. While the cost (i.e., effort) is easy to measure quantitatively, the benefit is usually hard to quantify. Therefore, we rely mostly on the subjective assessment of the benefits as seen from the risk management team.

In the following, we first describe the costs and benefits separately and then combine both aspects.

The cost of risk management can be measured in terms of the effort that is spent on the activities of the risk management process. Figure 8 shows the effort spent in this case study. In total, 23 person days were spent in total from the project team and facilitator team, which represents 5% of the overall effort for project management.

[2]Architects are senior developers responsible for the SW architecture

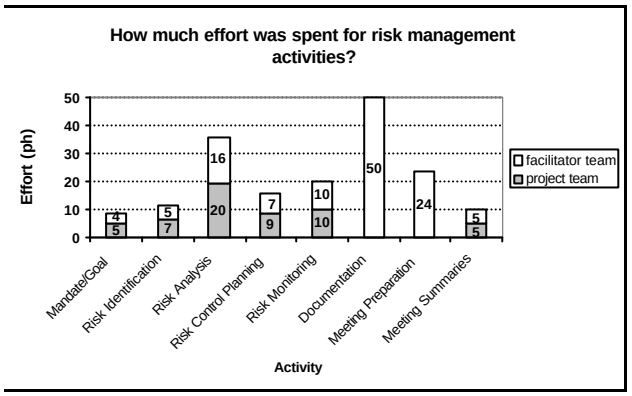


Figure 8: Effort spent on risk management

To assess the benefits of risk management, we collected quantitative measurement data on the number of risks, the number and effectiveness of the controlling actions as well as qualitative data in terms as the benefits subjectively seen by the participants.

In Figure 9, the number of risks identified and/or tracked in this project is shown over the project's time.

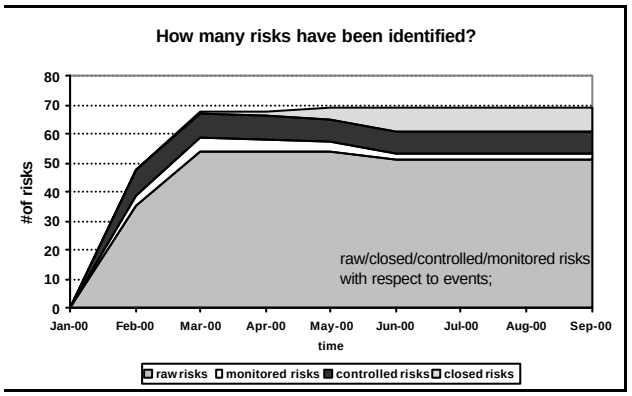


Figure 9: Number of Risks

It can be seen that the number of identified but not analyzed risks (i.e., raw risks) is quite large. Thus, a relatively small proportion of those risks identified during risk identification was considered during risk analysis. It can also be observed that no major risk identification took place after June. This can be attributed to problems in the project. Nevertheless, participants thought retrospectively that the controlled risks contained most of the project's important risks.

For the controlled risks Figure 10 shows the impact of the controlling actions on the risk. The risk management team assessed the impact subjectively on a scale of {high, medium, low, no impact, unknown impact}.

As can be seen, about 1/5 of the defined controlling actions showed high impact on preventing or reducing the risk. Thus, for these controlling actions it can be concluded that their implementation was valuable for the project as they effectively contributed to the mitigation of the corresponding risk.

On the other hand, it can also be seen that a large proportion of controlling actions is rated as *unknown impact*. This situation corroborates the above-mentioned finding that the impact of the controlling actions was not sufficiently questioned and that many controlling actions were not implemented as planned.

To foster qualitative assessment of the benefits of risk management, our questionnaire contained the question: *What was the overall impact of risk management on the project?*

Here, participants stressed the systematic and sound approach of an explicit risk management process that was definitely an improvement over the more intuitive risk management performed prior to the introduction of Riskit. Participants learned that it is possible to systematically identify risks and, even more important, successfully tackle them by means of controlling actions.

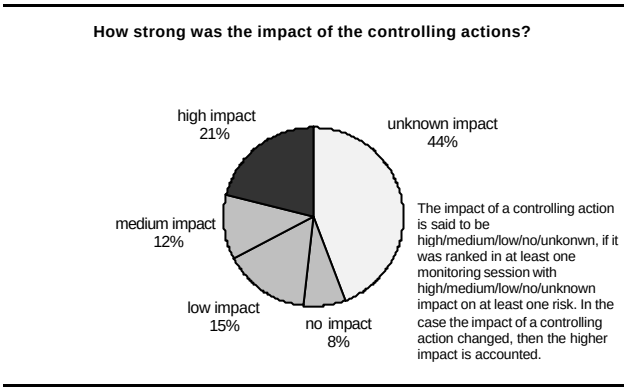


Figure 10: Impact of controlling actions

In order to decide whether risk management should be implemented in a new project within Tenovis or a new company, the ratio between cost and benefit has to be taken into account. Due to the qualitative nature of the benefits, the ratio can only be assessed subjectively. Therefore we asked the participants: *Considering the effort spent on risk management, the number of identified/controlled risks, and the impact of the controlling actions, would you say that the invested effort paid off?*

While the amount of effort was seen as acceptable by the participants, they regarded the impact of risk management on the project in this case study as too low. They rated the relationship between cost and benefit for the project as negative or neutral at best.

However, since the low impact of risk management on the project can be attributed to the weak implementation of the controlling actions, there is a clear potential for improving the cost-benefit in the future with the experience from this project.

On the other hand, at management level the existence of a more systematic and explicit risk management providing a more professional project management was seen as worth the cost.

Because of this and the prospect that improved risk management will also have a stronger impact on the project itself, management

will continue implementing explicit risk management using the concepts of Riskit in future projects.

Summarizing our findings related to the cost and benefit we can conclude:

- The cost of risk management accounted for 5% of the overall project management effort, which was seen as acceptable.
- At management level, the existence of more professional project management was seen as worth the cost.
- The impact of risk management on the project was seen as too low. With improved risk management, however, this impact can be improved respectively.

6.3 Comparison with Other Case Studies

In order to generalize the results of our study, we performed a cross-case analysis [34] and compared our findings with the findings of three earlier case studies investigating the Riskit method.

The first case study for Riskit, which was performed in 1996 at NASA [23][24], was an exploratory study for Riskit but also compared Riskit with a different method. In this study, the visual appeal and understandability of the Riskit analysis graphs was emphasized. Furthermore, this study found that users reported higher levels of confidence in the results of the Riskit method. Both of these findings seem to be in line with the overall feedback received from our study.

Additionally, the NASA study found that the Riskit method produced more detailed controlling actions. Although in our study, the Tenovis participants regarded the implementation of the controlling actions as weak, they, nevertheless, acknowledged that the controlling actions would have had a useful impact on the project if they had been implemented as planned.

In terms of effort, studies differ substantially: In the NASA study 20% of the management effort was spent on risk management, whereas in the Tenovis project this figure was 5%. One potential explanation for this difference could be the substantially smaller size of the NASA project. Another possible explanation could be the fact that the Riskit method itself was in its early development and perhaps contained more overhead activities during the NASA study.

The second study, which was conducted in 1998 at Nokia and DaimlerChrysler [27], evaluated the feasibility and usefulness of Riskit. Additionally, the study tried to identify issues related to the introduction of risk management. In this second study, the following observations were made:

- Motivation and clear definition of responsibilities are necessary for successful risk management.
- Project time pressures continually limit the time available for risk management.
- Systematic risk management was perceived as beneficial and seemed to improve participants' confidence in risk management results.

These findings are similar to the ones presented in this paper.

However, some findings differ. The DaimlerChrysler study indicated that users had difficulties understanding and using Riskit analysis graphs whereas in our study these graphs were considered very helpful. We believe that a major reason for this difference was the amount of training given to participants. In the DaimlerChrysler study, one to two hours of training were given to the risk management participants, whereas in the Tenovis study, a full-day workshop with exercises using material from the actual project was performed.

This explanation of factors impacting the understandability of the Riskit analysis graphs emphasizes our finding that appropriate training is essential for a successful technology transfer for Riskit.

The third study, which was performed by Getto and Landes in the context of DaimlerChrysler in 1999 [18], emphasized the need for efficiency in risk management. Again, this is similar to the findings of our study.

This third study also emphasized the importance of stakeholders as defined in Riskit (cf. Figure 2), a fact that was also reported in the second study performed at Nokia and DaimlerChrysler. In our study, the concept of stakeholders was not explicitly mentioned in the case study interviews by the interviewees. Yet, during the course of the project, discussions took place in the risk management team on stakeholders, their goals, and their goal priorities.

In summary, the findings in all four studies seem to be fairly consistent and the natural variance in the way the method was applied in the various contexts can be used to find more effective ways of applying the method.

7. LESSONS LEARNED FROM THE CASE STUDY

Based on the results reported above we developed a set of lessons learned that we consider the essentials of our case study. They are largely independent of the project and as such can be applied to other projects as well.

- *Explicit and systematic risk management is perceived as useful by project management.* Prior to Riskit's implementation the project managers performed most of the risk management activities, albeit in an informal and intuitive way. However, the explicit and systematic way was perceived as a valuable add-on to their daily practices.
- *The distinguishing features of Riskit were perceived as practical and understandable.* During risk identification, the combination of checklists and brainstorming allows both to include the experience and insight of the participants and, simultaneously, check systematically for typical risks. During risk analysis, the Riskit scenarios provided an effective way to understand and discuss about risks. During

selection of the most important risks, the Pareto table allows to take into account both the probability and utility loss effectively and comprehensibly even though they are measured by ordinal scale metrics.

- *Monitoring is one of the most important activities.* A vital prerequisite for successful risk mitigation is the ability to react quickly to changes in the status of a risk or its controlling actions, as early as possible. Risk monitoring on a *regular* basis is the key to this prerequisite. The method used for monitoring should be carefully selected to avoid tedious repetition, and the documentation should support the requirements of monitoring, as it is the activity that is performed most frequently.
- *Ensure seamless integration of risk management activities into the overall project work.* Regular project meetings should be used to perform the risk management activities. This is especially true for risk monitoring. Regular meetings enable participants to detect and react on changes in the status of risks or their controlling actions and prevents unnecessary overhead through additional meetings. Moreover, developers will not perceive risk management activities as additional burden but as part of their routine work. The integration should also force an appropriate level of documentation.
- *Ensure the commitment of the project manager when implementing risk management.* Although upper management often decides on the introduction of a technology such as risk management, the project manager is the one who, in the end has to make risk management decisions in the project and convince his or her project team. Therefore, the project manager's commitment is of crucial importance for successful technology transfer.
- *Process ownership of customized risk management process.* Although at the beginning of the technology transfer, the technology provider has the experience and competence with risk management, it is very important that the project manager takes over responsibility for the customized process. This ownership is necessary to adapt the process to the project's needs quickly and efficiently, and to perform the process in the most effective and systematic way. The role of the technology provider is to advise and support the project manager.

8. CONCLUSION

In this paper, we presented a case study of implementing risk management at Tenovis. The objectives of the case study were, on the one hand, to analyze the usefulness and adequacy of Riskit in order to tailor the method to Tenovis and improve it in general. On the other hand, the objective was to analyze the cost-benefit of Riskit in an industrial context.

Our results show that Riskit is a practical and understandable risk management method. Its techniques for describing risks (Risk Scenarios) and for selecting the most important risks (Pareto ranking technique) were highly appreciated by the risk management team.

While the costs for risk management were seen as acceptable, its impact on the project were, in this particular case, considered too low. Yet, the experiences from this case study can be used to improve risk management at Tenovis and thus increase its cost effectiveness. On a management, level the existence of a more professional project management was seen as worth the costs.

Additionally, we reported several lessons learned for both risk management in general, and Riskit in particular. They can be useful for all project managers who are considering the introduction of explicit risk management.

9. ACKNOWLEDGEMENTS

We would like to thank the participants of the Tenovis Risk Management Meetings for their commitment and their collaboration when we performed the case study interviews. Additionally, we would like to thank Sonnhild Namingha for proofreading the paper. Finally, we thank Ulrike Becker-Kornstaedt for her valuable comments on the contents and presentation of the paper.

10. REFERENCES

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

[2] Victor R. Basili, Gianluigi Caldiera, and H. Dieter Rombach, Experience Factory, in Encyclopedia of Software Engineering (John J. Marciniak, ed.), vol. 1, pp. 469-476, John Wiley Sons, 1994.

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

[4] Bezirkan, A. and Mulazzani, M. Experiences with Risk Management in a Large Multi-Site Project. 1994. Pittsburgh, PA, SEI. Proceedings of the Third SEI Conference on Software Risk Management.

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

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

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

[8] Briand, L. C., Differding, C., Rombach, D., Practical Guidelines for Measurement-based Process Improvement. Software Process - Improvement and Practice , Vol. 2, pp. 253 – 280, 1996.

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

[10] Carr, M., Kondra, S., Monarch, I, Ulrich, F., Walker, C., Taxonomy Based Risk Identification. 1993. Pittsburgh, PA, Software Engineering Institute. Technical Report CMU/SEI-93-TR-006.

[11] Chadbourne, B. C. To the Heart of Risk Management: Teaching Project Teams to Combat Risk. 1999. Proceedings of the 30th Annual Project Management Institute 1999 Seminars & Symposium.

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

[13] James W. DeLoach. *Enterprise-wide Risk Management -- Strategies for linking risk and opportunity*, Harlow, UK:Pearson Education Limited, 2000.

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

[15] Fairley, R., "Risk Management for Software Projects," *IEEE Software*, vol. 11, no. May, pp. 57-67, 1994.

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

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

[18] Getto, G. and Landes, D. Risk Management in Complex Project Organizations: A Godfather-driven Approach. 1999. Proceedings of the Project Management Institute (PMI) Conference 99.

[19] Groth, J. C., "Common-sense Risk Assessment," *Management Decision*, vol. 30, no. 5, pp. 10-16, 1992.

[20] Hall, E., M., Managing Risk. 1997. Addison Wesley, Reading, MA.

[21] Hefner, R. Experience with Applying SEI's Risk Taxonomy. 1994. Pittsburgh, PA, SEI. Proceedings of the Third SEI Conference on Software Risk Management.

[22] IEEE. Managing Risk. IEEE Software 14[3]. 1997.

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

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

[25] Kontio, J. The Riskit Method for Software Risk Management, version 1.00. CS-TR-3782 / UMIACS-TR-97-38. 1997. College Park, MD, University of Maryland. Computer Science Technical Reports. http://mordor.cs.hut.fi/~jkontio/riskittr.pdf

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

[27] Kontio, J., Getto, G., and Landes, D. Experiences in improving risk management processes using the concepts of the Riskit method. 163-174. 1998. Proceedings of the Sixth International Symposium on the Foundations of Software Engineering (FSE-6).

[28] Meyers, D. J. and Trbovich, D. R. One Project's Approach to Software Risk Management. 1993. Pittsburgh, PA, SEI. Proceedings of the Second SEI Conference on Software Risk Management.

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

[30] M.Q. Patton, Qualitative Evaluation and Research Methods, 2nd ed, SAGE Publications Inc., 1990

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

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

[33] Solingen, R. van, Berghout, E., The Goal/Question/Metric Method. 1999. London, McGraw-Hill.

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

[35] Wohlin, C.; Runeson, P.; Höst, M.; Ohlsson, M.; Regnell, B,; and Wesslen, A.; Experimentation in Software Engineering - An Introduction. The Kluwer International Series in Software Engineering, Kluwer Academic Publishers, 2000.