Fraunhofer Institut
Experimentelles
Software Engineering

An Industrial Case Study of Implementing Software Risk Management

Authors:
Bernd Freimut
Susanne Hartkopf
Peter Kaiser
Jyrki Kontio
Werner Kobitzsch

Submitted for for publication
at ESEC/FSE 2001

IESE-Report No. 016.01/E
Version 1.0
March 2001

A publication by Fraunhofer IESE

Fraunhofer IESE is an institute of the Fraunhofer Gesellschaft.
The institute transfers innovative software development techniques, methods and tools into industrial practice, assists companies in building software competencies customized to their needs, and helps them to establish a competetive market position.

Fraunhofer IESE is directed by
Prof. Dr. Dieter Rombach
Sauerwiesen 6
D-67661 Kaiserslautern

Abstract

Explicit risk management is gaining grounds 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 the 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 that wants to transfer risk management into new projects.

Keywords: Risk Management, Case Study, Lessons Learned, Riskit Method

Table of Contents

1	**Introduction**	**1**
2	**The Risk Management Method: Riskit**	**3**
3	**Case Study Context: The Project**	**6**
4	**Transfer of Risk Management**	**7**
5	**Case Study Design**	**9**
6	**Case Study Results**	**12**
6.1	Results for Riskit's usefulness	12
6.1.1	Usefulness/Adequacy of the Riskit Process	12
6.1.2	Instantiation of Risk Management at Tenovis	15
6.1.3	Adequacy of the Transfer	16
6.2	Results for the Cost-Benefit of Risk Management using Riskit	18
6.3	Comparison with other case studies	21
7	**Lessons Learned from the Case Study**	**23**
8	**Conclusion**	**25**
9	**References**	**26**

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][23]. Also, the increased requirements for risk management by many assessment standards have increased corporate interest in risk management.

The risk management practices have become much more operational and practical, as many guidelines and textbooks [21][14], as well as consultants, help organizations improve their risk management practices.

Yet, while the industry is clearly using risk management techniques more actively, there are 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 any specific attempt to scientific rigor or empirical research methods [29][31][4][9][17][18][11][36]. However, systematic empirical investigations are necessary to learn more about the transfer and application of risk management methods.

To contribute to this body of knowledge, this paper presents a case study on the implementation of a specific risk management method, namely the Riskit method, into the German company Tenovis, a key player in the telecommunication market.

The paper builds on a series of case studies related to the Riskit method [25][28][19]. The value of the 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 impacting the success of the transfer and implementation of risk management.

The objective of the case study presented in this paper was to (1) characterize the *usefulness and adequacy* of the *Riskit risk management process* from the viewpoint of the *risk management participants* and (2) to characterize the *cost-benefit* of the *Riskit risk management process* in the context of *Tenovis*.

The first objective was to identify effective ways of introducing risk management at the company in question and in general, and at providing feedback for improving the Riskit method. The second objective was to investigate the economic impact of the Riskit method.

The reminder 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: 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. As Riskit has been extensively presented in other publications [24][25][26][27][28], we present here only the highlights and main principles of the method.

Riskit contains is 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 [26].

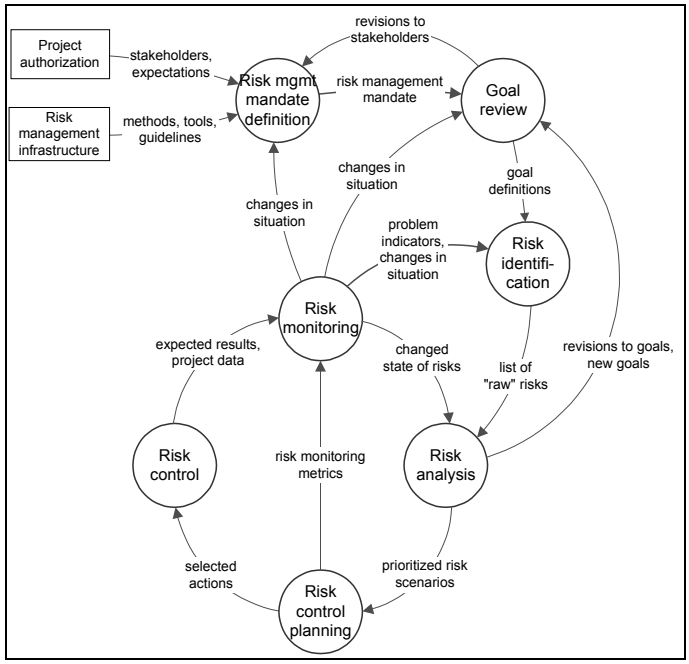


Figure 1: Overview on Riskit process

The Riskit process contains a specific step for analyzing stakeholder interests. 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.

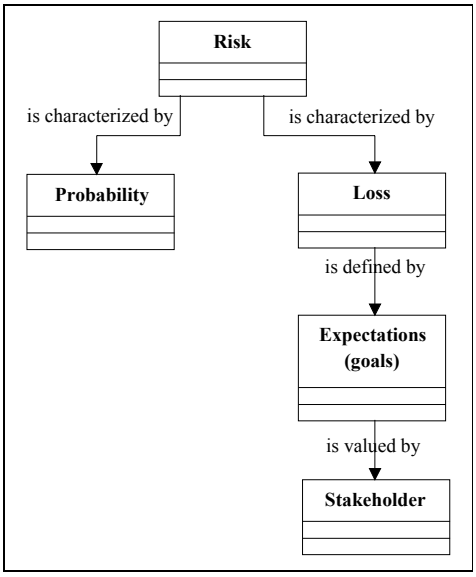


Figure 2: Definition of Risk within Riskit

When risk are defined, their impact to 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 their perspective.

The Riskit method supports unambiguous definition for 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 deeper, qualitative understanding of them.

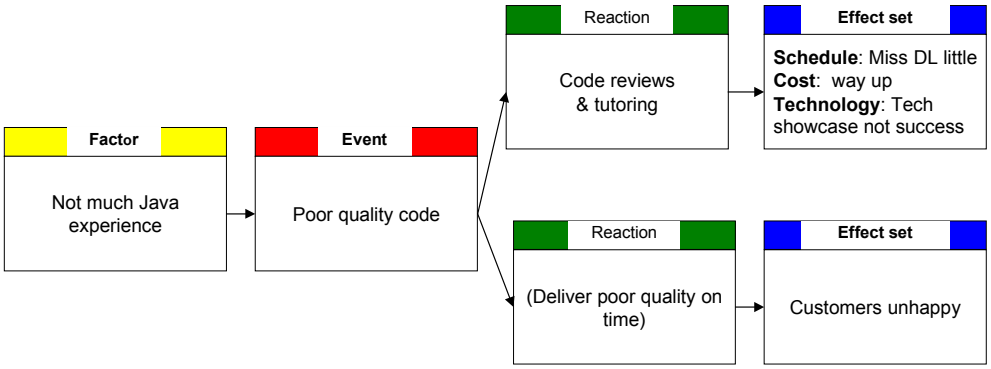


Figure 3: Example of the Riskit analysis graph (risk scenarios)

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 for probability and loss are seldom available and it is difficult to account for multiple goal effects and for the non-linear utility function.

Riskit largely avoids these problems by using ranking techniques that are matched to the type of information available. Expected utility loss calculations are used when ratio or distance scale data is available. However, when only ordinal scale metrics are available for probability or 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, whose evaluation is based on utility theory [3][16][17].

3 Case Study Context: The Project

Tenovis is a key player in the telecommunication market. As successor of Bosch Telecom, respectively Telenorma, it has about 8500 employees and more than 100 years of experience. Tenovis works in a wide range of telecommunication areas such as private branch exchanges (PBX), call centers, and IP-based telephony.

The project that is considered in this case study aimed at providing a unified, harmonized tool supporting the 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 last 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 for design and implementation was selected, a fact, which added complexity and increased demands for cost effectiveness to be mastered by the development teams. Beside the new technologies a new development processes and a new project organization were introduced, which involved teams from three different locations and time zones (India, France, and Germany).

In the early beginnings of the project, risk management was performed in an informal way. However, this intuitive risk management was considered as no 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 demands impose in general risks to telecommunication projects. Additionally, the introduction of new technologies and processes imposed also risks. Hence, this project was seen as particularly risky. 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) was selected as the basis for risk management. This 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 of a project. Risk management by experience enables learning from other projects by means of an experience factory [2].

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 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 5).

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.

This risk management team was supported by the authors from Fraunhofer IESE, who had the role of facilitators in the risk management meetings. In this role they prepared the meetings, for example, by selecting and preparing the risk management techniques to be applied, by providing the necessary documents, and by sending invitations. During the meetings they moderated the discussions and cared for the correct application of the risk management techniques. Additionally they were responsible for 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 on a regularly basis.

5 Case Study Design

The empirical study reported in this paper is a case study with predefined objectives and some level of control wrt. overall arrangements of the study. The fact that the authors themselves were part of the study also introduced aspects of action research [32], as the authors were able to observe 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 that are shown below.

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.

Under usefulness and adequacy we understand the advantages and drawbacks of risk management with respect to the (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 new technology.

Using the Goal-Question-Metric Paradigm [35][8] we refined these goals in questions characterizing the quality aspects usefulness, adequacy, and cost-benefit. Subsequently, we refined these questions in metrics defining the data to be collected to answer the questions and evaluate the research goals. The identified metrics were of two kinds: 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 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 em-

ployed 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 4) for a structured interview. Using these materials we interviewed all five members of the Tenovis risk management team, where each interview lasted about one hour. The interview was held with one interviewer and one scribe who recorded the interviewees' answers. The recorded answers were entered for a better analysis into a data base and sent to the interviewees for verification.

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.
   - ☞ after initial open question put figure on table to ask specifically for remaining ones
   - ☞ check with scribe for completeness of objectives and main benefits.

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

2. Considering the techniques applied in the process (see figure), which **techniques** were particular **useful** (and why?) and which techniques should be thought over (and why?)?
   - ☞ (esp.: risk identification: difference between brainstorming, checklists)
   - ☞ When the interviewee answers to the open question, the interviewer also tries to get answers to answers 10-16. Show concrete example then
3. ☞ Was this development of risks into **RiskIt-Scenarios helpful** for an understanding of the risk?
4. ☞ What do you think about the **documentation** of the risks as **RiskIt Scenarios**? (was appropriate, too laborious)?
5. ☞ Did you have **appropriate information to perform this comparison** to identify the worse or more likely scenario? (if not: what was missing or difficult?)
6. ☞ Was the selection of TOP10 risks using the **Pareto table** comprehensible (nachvollziehbar) or were there problems?(If not: which problems?)
7. ☞ Were the **monitoring questions** useful for determining a risk's and the project's status?
8. ☞ Was the **information on the risk sheet** appropriate for risk monitoring?
9. ☞ In general, was the **level of detail for documenting** the risks in the risk scenario forms too much, enough, not enough?
10. Considering the risk management process, where there any **steps** in which in your point are **improvement potentials**. If yes, in which step and what can be done better?

Figure 4: Excerpt of interview procedure

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

To improve the risk management process and to better tailor it to the environment, we devised a set of improvement suggestions.

To verify our conclusions and suggested process improvement proposals a feedback session with the members of the risk management team (i.e., the in-

terviewees) 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 validity threats that make it difficult to control the quality of the study and to generalize their result [34][37]. In the following we describe how we took specific steps to minimize the impact of three kinds of validity threats.

Observation and facilitator bias was reduced by emphasizing Tenovis participant feedback, using the interviewing procedures described earlier, and by carefully discussing and evaluating the facilitator observations and findings. Also, we kept logbooks after each meeting to record out observations in their original form.

The *selection* of the sample of participants in the project was representative, as most key people in the management participated in risk management actions. As discussed earlier, 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 one hand this may have biased the participants to recognize the need for risk management more clearly, on the other hand the pressures of aggressive goals may have also reduced the time available for risk management activities, increasing the expected cost-benefit of the risk management process.

It is likely that the *maturation effect* influenced the results as well, i.e., participants became more fluent in risk management over time and, therefore, their later opinions – when the interviews took place – may have been more positive than they would have been in the beginning. We believe that this effect is inconsequential as all participants were just going up their learning curve on risk management. In future projects they will already possess the improved risk management experience.

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 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. In Section

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 single activities 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 at the beginning risks are unsystematically identified and not appropriately tracked, the process triggers all necessary activities. A 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 systematic and comprehensive. Retrospectively the participants regarded that most of the project's risks were identified during risk identification. Additionally, the composition of the risk management team with people from different roles (i.e., people with a different view on the project) was beneficial, as the different views on potential risks and 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 communicate about risks.

These Analysis Graphs were rated as very helpful in understanding the risk, its context, and consequences. A 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 (a discussion of a risk event and developing the corresponding scenario took about 17min on average) the 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 received 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. The selection of the most important risks was performed by means of a Pareto-table [26]. This selection was regarded as comprehensible and thus the 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 5).

Tenovis Risk Scenario Form

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

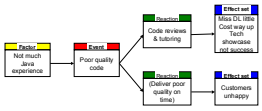
Potential risk controlling actions: Improve review practice, organize tutoring – log results, define metrics and thresholds, reduce time pressure and communicate importance of quality

Selected risk controlling actions

	Action	*Respons.*	*State*	*Finish*	*Check*
1	Introduce review process	Smith	done	end May	✓
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	✓
5	Communicate importance of quality	Miller	done	end Sep	✓

Closing date: **Closing Rationale**:

Graphical representation of scenario



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 5: Risk Scenario Form for one risk event

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 many contents for daily work, especially for risk monitoring. During risk monitoring the participants were 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, the risk management team became new members in the course of the project. 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, that it complicates the re-use of risk experience in future projects.

Third, the effort of the documentation was considered as too high (cf. Figure 6) After a risk monitoring meeting, which was to be performed bi-weekly, the facilitator team spend about two hours on updating the statuses of the controlling actions as well as the risks' and controlling actions' 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. Especially the distinguishing features of Riskit were regarded as particularly valuable.

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 was retrospectively seen as a drawback as 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 the risk management.

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

Risk Monitoring: Risk Monitoring is one of 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 a 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 risks' and controlling actions' statuses. Moreover, due to the long intervals it was difficult for the participants to remember the context of the risks and their controlling actions.

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

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 considered that the controlling actions were not performed as planned and therefore were not effective as they could have been. This could have been prevented by a stronger questioning of the controlling action. Thus, in the future the implementation of the controlling action (what?) and its impact on the risk (how good?) has to be stronger 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 meeting.
- Risk monitoring has to sufficiently question the implementation of controlling actions and their impact on the risk.

6.1.3 Adequacy of the Transfer

To assess the adequacy of the technology transfer the questionnaire contained the questions How did you perceive the work split between Tenovis and IESE? and From your point of view, how the was commitment for risk management from the {architects, 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 tutorial but also the developers. The purpose is on one hand to enable also the developers for risk management activities (as risk management is more to be included in the project work). On the other hand the tutorial can also raise the awareness for risk management and risks.

Process Ownership: As described in section 4, the technology was transferred by the authors from IESE performing the entire facilitation in the meetings and maintaining the documentation. The facilitators also triggered the risk man-

agement 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, the process ownership was actually with the facilitators and not with the project management team or even the Tenovis company. Consequently, the 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 heed the 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 includes therefore also activities that arise from controlling actions, and the motivation of 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 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 Risk Management using 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 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 6 shows the effort spent in this case study. In total, 17 person days were spent on risk management, which represents 3% of the overall effort for project management.

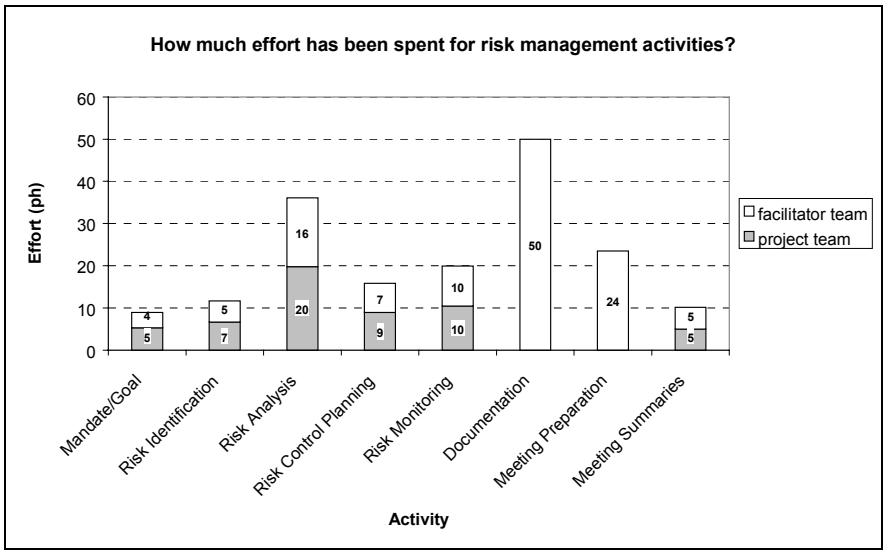


Figure 6: Effort spent on risk management

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

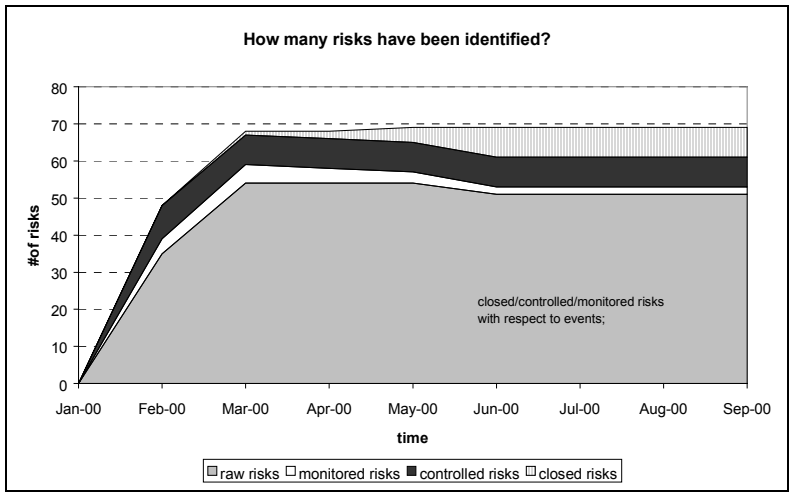


Figure 7: Number of Risks

It can be seen that the number of identified but not analyzed risks (raw risks, i.e., identified, but not yet analyzed risks) is quite large. It can also be observed that no major risk identification took place after June. This can be contributed to problems in the project. Nevertheless, the participants considered retrospectively that the controlled risks contained most of the project's important risks.

Figure 8 shows for the controlled risks 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}.

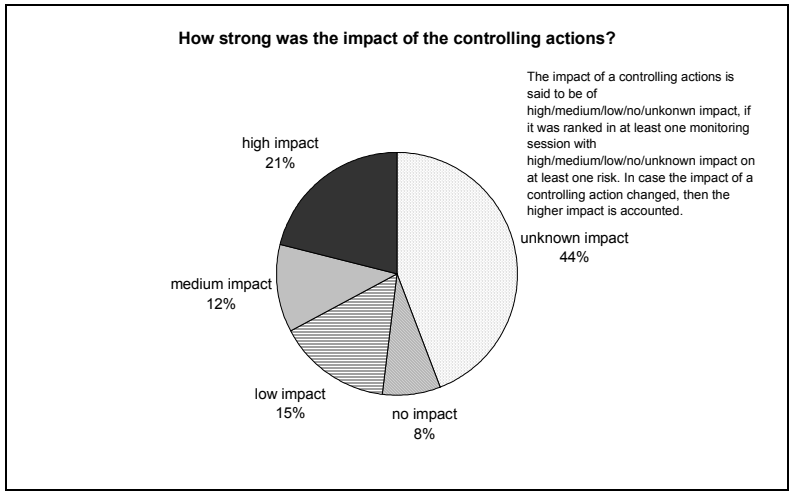


Figure 8: Impact of controlling actions

As it can be seen about 1/5 of the defined controlling actions showed a 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 the 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 the 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. The participants learned that it is possible to systematically identify risks and, even more important, successfully tackle them by means of controlling actions.

In order to decide whether risk management should be implemented in a new project within Tenovis or whether it is worth implementing in a new company, the ratio between cost and benefit has to be taken into account. Due to the qualitative nature of the benefits, also the ratio can only be subjectively assessed. 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 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 as negative or neutral at best.

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

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

This fact and the prospect that an 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 3% of the overall project management effort, which as seen as acceptable.
- On a management level the existence of a more professional project management was seen as worth the costs.
- The impact of risk management on the project was seen as too low. With an 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 compare our findings with the findings of three earlier case studies investigating the Riskit method.

The first case study for Riskit, which was performed 1996 at NASA [24][25], was an exploratory study for Riskit and 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 level 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. Thus, again our findings are in line with the NASA study.

In terms of effort, both 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 3%. A potential explanation for this difference could 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 study at Nokia and Daimler-Chrysler [28], 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 to successful risk management.
– Project time pressures continually limit the time available for risk management.

– The systematic risk management was perceived beneficial and seemed to improve participants' confidence in risk management results.

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

However, some findings differed. The second study indicated that users had difficulties in understanding and using Riskit analysis graphs. We believe that a major reason for this difference was the amount of training given to participants. In the second 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 for 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 [19], 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, 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, in the course of the project discussions in the risk management team on stakeholders, their goals, and their goal priorities took place.

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 case study results reported above we can come up with a set of lessons learned that we consider the essentials of our case study. They are largely independent from 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 about understanding and communicating about risks. During the selection of the most important risks the Pareto-table allows effectively and comprehensibly to take into account both the probability and utility loss even though they are measured by ordinal scale metrics.
- *Monitoring is one of the most important of the activities.* A vital prerequisite for successful risk mitigation is the ability to react quickly to changes in this risks' or controlling actions' statuses as early as possible. Risk monitoring on a regular basis is the key to fulfill 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 which is performed most frequently
- *Care for a seamless integration of risk management activities in the overall project work.* Regular project meetings should be used to perform the risk management activities. This is especially true for risk monitoring. This enables the participants to detect and react on changes in the risks' or the controlling actions' status and prevents unnecessary overhead through additional meetings. Moreover, the developers will not perceive the risk management activities as additional burden but as part of their routine work. The integration should also force an appropriate level of documentation
- *Care for the commitment of the project manager when implementing risk management.* Although often-upper management decides about the introduction of a technology such as risk management, the project manager is the one who finally has to take the risk management decisions in the project and to convince his or her project team. Therefore, the project man-

ager's commitment is of crucial importance for a successful technology transfer.

– *Process ownership.* 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 process ownership is with the project manager. The role of the technology provider is to consult 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 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 it was the objective 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, the impact of it on the project were in this particular case considered as too low. Yet, the experiences from this case study can be used to improve the 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 considering the introduction of explicit risk management.

9 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, 1989a.

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

[18] 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.

[19] 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.

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

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

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

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

[24] 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.

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

[26] 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

[27] 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.

[28] 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).

[29] 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.

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

[31] Morin, J.-M. Risk Driven Project Management: A Practical Approach. 1993. Pittsburgh, SEI. Proceedings of the Second SEI Conference on Software Risk Management.

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

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

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

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

[36] Williamson, J. A. Experiences with an Independent Risk Assessment Team. 1994. Pittsburgh, PA, SEI. Proceedings of the Third SEI Conference on Software Risk Management.

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

Document Information

Title:	An Industrial Case Study of Implementing Software Risk Management
Date:	March, 2001
Report:	IESE-016.01/E
Status:	Submitted
Distribution:	Public