Chapter VI
Building IT Risk Management Approaches:
An Action Research Method

Jakob Holden Iversen
University of Wisconsin Oshkosh, USA

Lars Mathiassen
Georgia State University, USA

Peter Axel Nielsen
Aalborg University, Denmark

ABSTRACT

This chapter shows how action research can help practitioners develop IT risk management approaches that are tailored to their organization and the specific issues they face. Based on literature and practical experience, the authors present a method for developing risk management approaches to use in real-world innovation projects. The chapter illustrates the method by presenting the results of developing a risk management approach for software process improvement projects in a software organization.

INTRODUCTION

Organizations that manage IT innovations have long been accused of having poor project execution and low product quality. These problems are often referred to as "The Software Crisis," in which software projects frequently are delivered late, over budget, with missing features, and with poor quality. Furthermore, it has been very difficult to predict which organization would do a good job on any given project. These issues led to the establishment of the software process improvement (SPI) movement, in which poor processes in organizations are considered a major reason for the software crisis.

Organizations routinely rely on experienced developers to deliver high quality IT systems. However, in the 1990s, organizations realized that by defining and improving the processes these professionals used, it was possible to deliver more consistent results with better quality. SPI projects were established to improve specific aspects of a process, and in many cases to take advantage of standards like the Capability Maturity Model (CMM) (Paulk et al., 1993) and the Capability Maturity Model Integration (CMMI) (Chrissis et al., 2003). For each process that needed improvement, a focused SPI project would design and implement specific improvements into current practices.

However, not only is this hard work, it also is risky business. Much can go wrong in improvement projects, and mistakes can eventually lead to failure. The involved improvement actors might not possess appropriate skills and experiences. The design of a new process might not suit the organization or effectively meet requirements. The improvement project might be organized inappropriately, with unrealistic schedules or insufficient management attention. Also, the actors might pay too little attention to customers, failing to consider the interests, problems, and motivations of the people and groups that are expected to use the new process.

To deal proactively with such issues in SPI projects, the involved actors must manage the involved risks. The need for such risk management was the rationale behind Danske Bank's development of a practical risk management approach to reduce failures in their SPI initiative. Using this approach, improvement actors periodically held disciplined and tightly structured workshops in collaboration with SPI facilitators. The workshops gave each team a better overview and understanding of their project and its organizational context, and helped them address risks proactively.

Organizations face many different and quite diverse activities in which there are strong reasons to manage IT risks. While the literature provides a portfolio of IT risk management approaches that cover many types of activities, organizations often face situations in which they need to develop a risk management approach that is tailored to their particular needs or that addresses issues not covered by the available portfolio of documented risk management approaches. This chapter offers organizations a generic method to develop new and dedicated IT risk management approaches. The method is based on action research into an organization's specific risk management context and needs, and builds on the available literature about IT risk management. It is based on our experiences from developing the tailored approach to risk management in SPI projects at Danske Bank.

RISK MANAGEMENT LITERATURE

A number of different approaches to IT risk management have been proposed. In this section, we provide an overview and categorization of the different approaches (risk list, risk-action list, risk-strategy model, risk-strategy analysis). We offer, in this way, a framework to help select an appropriate risk approach suited to particular organizational contexts and needs. An overview of the framework is shown in Table 1.

Risk List

The first and simplest form of available approaches are risk lists. They contain generic risk items (often prioritized) to help managers focus on possible sources of risk; they do not contain information about appropriate resolution actions. These lists are easy to use in assessing risks; they are easy to build, drawing upon published sources on risks or experiences within a particular context; and they are easy to modify to meet conditions in a particular organization or as new knowledge is captured. While these approaches offer strong support to help managers appreciate risks, they

Table 1. Four types of approaches to IT risk management

Type of Approach	Characteristics	Assessment E	xemplars
Risk list	A list of prioritized risk items +	Easy to use + Easy to build + Easy to modify + Risk appreciation - Risk resolution - Strategic oversight	(Barki et al., 1993; Keil et al., 1998; Moynihan, 1996; Ropponen & Lyytinen, 2000)
Risk-action list	A list of prioritized risk items with related resolution actions	+ Easy to use + Easy to build + Easy to modify + Risk appreciation + Risk resolution - Strategic oversight	(Alter & Ginzberg, 1978; Boehm, 1991; Jones, 1994; Ould, 1999)
Risk-strategy model	A contingency model that relates aggregate risk items to aggregate resolution actions	+ Easy to use - Easy to build - Easy to modify + Risk appreciation + Risk resolution + Strategic oversight	(Donaldson & Siegel, 2001; Keil et al., 1998; McFarlan, 1981)
Risk-strategy analysis	A stepwise process that links a detailed understanding of risks to an overall risk management strategy	- Easy to use - Easy to build + Easy to modify + Risk appreciation + Risk resolution + Strategic oversight	(Davis, 1982; Mathiassen et al., 2000)

do not support identification of relevant resolution actions and they do not provide a strategic oversight of the risk profile and relevant strategies for action. Based on previous research, Barki et al. (1993) offer a detailed and precise definition, a measure of software development risk, and a systematic assessment of the reliability and validity of the instrument. Moynihan (1996) presents a comprehensive list of risk items based on how software project managers construe new projects and their contexts. Keil et al. (1998) offer a list of nearly a dozen risk factors that IT project managers in different parts of the world rated high in terms of their importance. Ropponen and Lyytinen (2000) report six aggregate risk components, for example, scheduling and timing risks, that experienced IT project managers found important in a recent survey.

Risk-Action List

The second, slightly more elaborate, form of approaches are risk-action lists. They contain generic risk items (often prioritized), each with one or more related risk resolution actions. They also are easy to use; they are quite easy to build, but compared to risk lists, they require additional knowledge of the potential effects of different types of actions; finally, they are easy to modify when needed. Risk-action lists offer the same support as the risk lists to appreciate risks. In addition, they adopt a simple heuristic to identify possible relevant actions that might help resolve specific risks. However, by focusing on isolated pairs of risk items and resolution actions, they do not lead to a comprehensive strategy for addressing the risk profile as a whole. Alter and Ginzberg (1978) list eight risk items related to IT system implementation, for example, unpredictable im-

pact; and they offer four to nine actions for each risk, for example, use prototypes. Boehm (1991) offers a top-ten list of software development risks, with three to seven actions per risk. Jones (1994) presents specialized risk profiles for different types of IT projects, together with advice on how to prevent and control each risk. Finally, Ould (1999) suggests maintaining a project risk register for identified risks, assessment of the risks, and risk resolution actions to address them.

Risk-Strategy Model

The third form of approaches are risk-strategy models. These contingency models relate a project's risk profile to an overall strategy for addressing it. They combine comprehensive lists of risk items and resolution actions with abstract categories of risks (to arrive at a risk profile) and abstract categories of actions (to arrive at an overall risk strategy). The risk profile is assessed along the risk categories using a simple scale (e.g., high or low), which makes it possible to classify a project as being in one of a few possible situations. For each situation, the model then offers a dedicated risk strategy composed of several detailed resolution actions. Compared to the other types, risk-strategy models provide detailed as well as aggregate risk items, and resolution actions. The heuristic for linking risk items to resolution actions is a contingency table at the aggregate level. Risk-strategy models are easy to use because of the simplifying contingency model, but they are difficult to build because the model must summarize multiple and complex relationships between risks and actions. They also are difficult to modify except for minor revisions of specific risk items or resolution actions that do not challenge the aggregate concepts and the model. Models like these help appreciate risks and identify relevant actions, and managers can build an overall understanding of the risk profile they face (at the aggregate level) directly related to a strategy for addressing it (in terms of aggregate actions).

The best known of these approaches is McFarlan's (1981) portfolio model linking three aggregate risk items (project size, experience with technology, and project structure) to four aggregate resolution actions (external integration, internal integration, formal planning, and formal control). Keil et al. (1998) present a model that combines the perceived importance of risks with the perceived level of control over risks. The model suggests four different scenarios (customer mandate, scope and requirements, execution, and environment) with distinct risk profiles and action strategies. Donaldson and Siegel (2001) offer a model categorizing projects into a high, medium, or low risk profile. They suggest a different resource distribution between project management, system development, and quality assurance, depending on a project's risk profile.

Risk-Strategy Analysis

The final form of approaches are risk-strategy analyses. These approaches are similar to risk-strategy models in that they offer detailed as well as aggregate risk items and resolution actions, but they apply different heuristics. There is no model linking aggregate risk items to aggregate resolution actions. Instead, these approaches offer a stepwise analysis process through which the involved actors link risks to actions to develop an overall risk strategy. Compared to the risk-strategy models, there is a looser coupling between the aggregate risk items and aggregate resolution actions. In comparison, we find these approaches more difficult to use because they require process facilitation skills. They are as difficult to build as the risk-strategy models, but they are easier to modify because of the loosely defined relationship between aggregate risk items and resolution actions. Davis (1982) provides such a stepwise approach to address information requirements risks where the overall level of risk is assessed and then associated with four different strategies to cope with requirements uncertainty.

Mathiassen et al. (2000) offer a similar approach to develop a risk-based strategy for object-oriented analysis and design.

The comparative strengths and weaknesses of these four risk approaches are summarized in Table 1. Comparing the list approaches and the strategy approaches suggests that the former are easier to use, build, and modify, whereas the latter provide stronger support for risk management. Comparing risk-strategy models and the risk-strategy analysis approaches suggests that the former are easier to use, but they require that a contingency model be developed. The latter are easier to modify because they rely on a looser coupling between aggregate risk items and resolution actions. Organizations can use the insights in Table 1 to choose appropriate forms of IT risk management that are well suited to the particular challenges they want to address.

ACTION RESEARCH

Action research allows practitioners and researchers to interact with a real-world situation gaining deep insights into how an organization functions and how different interventions affect the organization. At the same time, it allows practitioners to reflect on their practice and gives them strong tools to improve their current situation (Checkland, 1991; McKay & Marshall, 2001). Along similar lines, Schön (1983) refers to the reflective practitioner that is informed by research, allowing researchers sometimes to act as practitioners and practitioners sometimes to act as researchers. We propose a modified action research approach, called collaborative practice research (CPR) that is appropriate for developing risk management methods by reflective practitioners or by collaborative groups of practitioners and researchers (Iversen et al., 2004; Mathiassen, 2002).

At Danske Bank, the cyclic nature of action research combined theory and practice as follows. The research interest and practical problems we faced were about SPI and how SPI teams can manage risks. The practical setting in which we addressed risk management was the SPI teams in the IT Department of Danske Bank (the largest Danish bank). The purpose here was to improve the SPI Teams' handling of SPI-related risks. Within this area we applied and combined theories and concepts about SPI and IT risk management. The result of this cyclic process was double: an approach to manage SPI risks in Danske Bank and a generic method for developing risk management approaches. The approach to manage SPI risks is presented in the section *Managing SPI Risks*, while the generic method for developing tailored risk approaches is presented in the rest of this section, based on the cyclic process of action research.

Our method to developing risk management approaches is illustrated in Table 2. It addresses a particular area of concern and is supported by risk management knowledge. The method provides an iterative approach to develop a tailored risk

Table 2. Developing risk management approaches

Initiating
1. Appreciate problem situation
2. Study literature
3. Select risk approach
Iterating
4. Develop risk framework
5. Design risk process
6. Apply approach
7. Evaluate experience
Closing
8. Exit
9. Assess usefulness
10. Elicit research results

management approach through application to a real-world situation in a specific organizational context, as shown in Table 2.

The proposed method is based on the ten activities of a CPR process (cf. Table 2), and consists of three phases: Initiating (activities 1 to 3), Iterating (activities 4 to 7), and Closing (activities 8 to 10). The sequence between activities 4 and 5 may not hold in practice, and only points to the logical dependencies between the activities. The sequence from 4 to 7 is based on the canonical problem-solving cycle (Susman & Evered, 1978). The iterating phase leads to risk management within the area of concern. The closing phase produces a refined risk management approach, together with an assessment of its usefulness.

The actors in this process enter the problem situation, bringing in prior experience and knowledge of the area of concern (activity 1). The actors should: (1) have experience within the area; (2) perceive the situation as problematic; and (3) find out to what extent and in which way risk management would be beneficial. Part of this activity is to assess whether these prerequisites are met and to establish a project with goals and plans to develop a tailored risk management approach. Activity 1 leads to an appreciation of the risk items and resolution actions perceived to be important within the area of concern (SPI in our case). Activity 2 uses the relevant risk management literature to complement activity 1 and leads to a comprehensive set of risk items and resolution actions that are used in activity 4. The type of risk approach is selected in activity 3 (cf. Table 1), based on the desired features of the approach and the characteristics and needs of the organizational context. This choice defines the basic structure of the risk management approach to be developed.

Activity 4 aggregates the identified risk items and resolution actions into a risk framework of the area of concern (see section *Managing SPI Risks*). Then a risk process is developed in activity 5. The process is based on the framework and on specific risk items and resolution actions. The risk approach is applied subsequently to specific situations or projects within the area of concern (activity 6). This leads to risks being managed and to experiences using the new approach (activity 7).

The iterating phase ends when the actors agree that the risk management approach is developed sufficiently and the problems in the area of concern are alleviated (activity 8). Whether the applications of the risk management approach were useful in practice is assessed relative to the problem situation at hand (activity 9). A simple way to do this is to ask the participants in the risk assessment if they found the risk management approach useful and to document whether risk management led to actions and improvements. The ways in which the new risk management approach contributes to the discipline in general are assessed relative to the relevant body of knowledge (activity 10).

We suggest that this method can be used in different contexts within information systems and software engineering. In adopting the method, actors are advised to consider specific criteria that will help them achieve satisfactory relevance of the outcome and sufficient rigor in the process. Actors are, as described, advised to use the framework of IT risk management approaches in Table 1 to guide their design.

CASE: RISK MANAGEMENT APPROACH IN SPI

This section presents the action research project that forms the basis for this research. It explains how we used the proposed method to develop a specific risk management approach and how this approach works.

Case Organization

This action research project was conducted at Danske Bank's IT Department, Danske Data,

Table 3. Action research performed by practitioners and researchers

Activities (see Table 2)	Initiating 10.97-12.97	First iteration 01.98-02.98	Second iteration 03.98-08.98	Third iteration 09.98-11.98	Fourth iteration 11.98-02.99	Closing 02.99-02.00
1. Appreciate problem situation	Part of on-going research collaboration [p1-4; r1-4] Brainstorm risk items and actions [p1-4; r1-4]					
2. Study literature	Study SPI [p1-4; r1-4] Study risk management [r1-2]					
3. Select risk approach	Synthesis [r1-3]	Confirmed selection [r1-3]		Appreciation of actors' competence [r1-3]		
4. Develop risk framework		Synthesis [r1-3] Review of framework of risk items and actions [r3] Revised framework [r1-3]				
5. Design risk process		List of risk items and actions [r1-3] Strategy sheets [r1-3]	Additional step and items reformulated [r2-3]	Improved documentation scheme [r1-3]		
6. Apply approaches		Risk assessment of Quality Assurance [p5-7; r2-3]	Risk assessment of Project Management [p3-4; r1-2]	Risk assessment of Metrics Program [p2; p8; r3]	Risk assessment of Diffusion [p9-10; r4; r3]	
7. Evaluate experience		Lessons learned [p5-7; r2-3]	Lessons learned [p3-4; r1-2]	Lessons learned [p2; r3]	Lessons learned [p9-10; r4; r3]	
8. Exit			Delay after 2nd iteration			Action part closed
9. Assess usefulness			Assessment of first two projects [p1-4; p11; r1-4]	Discussion of risk approach at CPR workshop [r1-r3]		Assessment of Metrics and Diffusion projects [p1-4; r1-4]
10. Elicit research results						Result and lesson elicitation [r1-3]

which was spun into an independent company, with Danske Bank as its primary customer. As the IT department began as part of the bank's accounting department, the traditional rigor of banking procedures still pervaded the culture to some extent. This had diminished somewhat in recent years as emerging technologies and the strategic role of IT to the bank's business became increasingly important.

Danske Bank joined a larger CPR (Mathiassen, 2002) project in 1997 (Mathiassen et al., 2002), aimed at implementing SPI projects in the participating organizations. Danske Data established a software engineering process group (Fowler & Rifkin, 1990) to manage and coordinate the SPI effort, which management clearly had articulated was intended to improve productivity (Andersen, Krath et al., 2002). The action researchers joined the SPI effort, along with a dedicated project manager, a consultant from the Methodology Department, and two information systems managers. One of the first activities conducted was a maturity assessment to determine which areas to target for improvement (Iversen et al., 1998). The assessment identified seven improvement areas. Subsequently, action teams were established to address each of these areas. As their work got underway, it became clear that there was a need to manage the inherent risks in conducting these organizational change projects. Danske Data called on the action researchers, who had extensive experience with risk management, to develop an approach to manage the risks faced by each of the SPI action teams. To satisfy the request, the action researchers embarked on the project described here, which eventually led to development of the method described in the previous section as well as the risk management approach for SPI described briefly in the Managing SPI Risks section and more fully in Iversen et al. (2002, 2004).

Action Research Project

The project was structured around four iterations, as described previously in Table 2. This section describes in detail how each iteration was conducted and what was learned. The effort involved 10 practitioners and 4 researchers (3 of whom are the authors). Table 3 illustrates a timeline of the four iterations and the involved actors and activities that took place in each. Most of the activities for this project took place between October 1997 and February 1999. Generally, the project was carried out in an iterative fashion, where risks and actions were identified in a bottom-up fashion and with practitioners and researchers collaborating closely on developing and testing the approach.

The project was initiated with a workshop that identified the risks and resolution actions that practitioners and researchers thought were the most important for SPI. When the workshop was conducted, the SPI project had been on-going for approximately one year, and both researchers and practitioners had significant practical experience with conducting SPI projects. Prior to the workshop, the practitioners worked through an existing SPI risk analysis approach (Statz et al., 1997), but found this approach too unwieldy and not sufficiently relevant to Danske Data. At the workshop, the researchers presented classical approaches to IT risk management (Boehm, 1991; Davis, 1982; McFarlan, 1981), after which the entire group conducted two brainstorms to determine risks and potential resolution actions that were relevant to SPI in Danske Data. Both of the resulting lists were very long and detailed (31 risk items and 21 resolution actions), which made them difficult to use. We obviously needed more structure.

Following the workshop, the authors studied the risk management literature and identified four types of approaches (Table 1). We chose to adopt a risk-strategy analysis approach, inspired by Davis (1982), for several reasons: We chose a strategy approach over a list approach because the

practitioners explicitly stated that they wanted an approach that could help them obtain an overall, strategic understanding of each SPI project. We chose the risk-strategy analysis approach over the risk-strategy model approach for two reasons. First, the stepwise analysis approach would help each SPI team obtain a shared, detailed understanding of risks and possible actions. Second, we were not confident that we would be able to develop a contingency model that would summarize the many different sources of risks and ways to address them in SPI. The action research subsequently went through four full iterations before closing.

First Iteration

Based on the lists of risk items and resolution actions from the workshop and insights from the SPI literature, the authors synthesized the brainstorms and developed a prototype of the risk management approach. A key challenge was developing a framework to understand risks and actions (see Figure 1 and Table 4). We further developed our initial classifications through a detailed examination of risk items and resolution actions mentioned in the SPI literature (Grady, 1997; Humphrey, 1989; McFeeley, 1996; Statz et al., 1997). The resulting risk management process was based on detailed lists of risk items and resolution actions for each of the four categories in the framework, and designed similarly to Davis' (1982) risk management approach (Iversen et al., 2004). Finally, we designed strategy sheets and simple scoring mechanisms to encourage a group of actors to engage in detailed risk and action assessments as a means to arrive at an informed, strategic understanding of how to address risks.

To test the approach, we arranged a workshop with the three practitioners responsible for improving quality assurance. We presented the risk framework and the process, but let the practitioners themselves apply the process, assisting only when they got stuck. The main experience was that the basic idea and structure of the approach was useful. However, during this first trial session, we only had time to cover half of the risk areas. The practitioners suggested that the process needed to be facilitated and managed by someone trained in the process, for example, the researchers. The practitioners found it especially difficult to interpret the questions in the risk tables in the context of their specific project. Some of the risk items needed to be reworded. Finally, to ease the interpretation of the risk items, the session should have started with an interpretation of the general terms in Figure 1 in the particular SPI context.

Figure 1. Risk areas for SPI teams

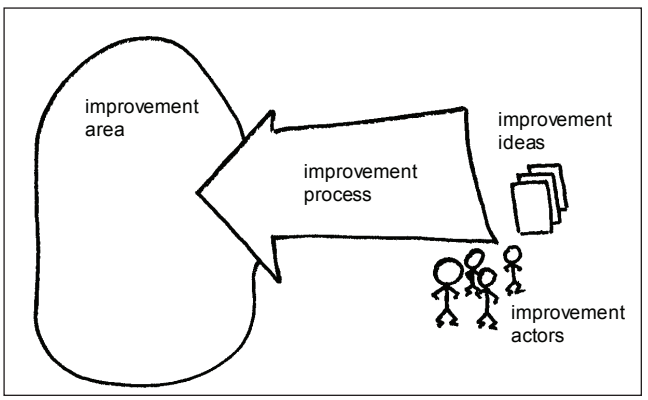

Table 4. Risk resolution strategies for SPI teams

Type of action C	*oncern*
1. Adjust Mission	What are the goals of the initiative? Goals may be adjusted to be more or less ambitious, e.g., targeting only projects developing software for a specific platform.
2. Modify Strategy	What strategy is the initiative going to follow? Covers the approach to develop the process as well as to roll it out in the organization. Roll-out may, for instance, follow a pilot, big bang, or phased approach.
3. Mobilize	From what alliances and energies can the initiative benefit? The likelihood of success of an improvement initiative can be improved significantly by adjusting which organizational units and actors are involved and by increasing their commitment.
4. Increase Knowledge	On which knowledge of software processes and improvement is the initiative based? Knowledge can be increased by educating team members, by including additional expertise into the team, or by hiring consultants.
5. Reorganize	How is the initiative organized, conducted, and managed? Covers organizing, planning, monitoring, and evaluating of the initiative.

Second Iteration

In the second iteration, we reworded the risk items and introduced a first step in which the SPI team should interpret the risk model in Figure 1 in their particular context. Then we performed a risk analysis with the two SPI practitioners responsible for improving project management. Both practitioners were skilled project managers with experience in risk management. The session included a complete risk analysis with identification of key risks and resolution strategies. The participating practitioners and researchers agreed upon the major lessons. First, the framework and the process assisted even skilled project managers through a more disciplined analysis than they usually would do on their own. Second, it would be advantageous to document the interpretations of specific risk items and resolution actions continuously throughout the workshop.

At subsequent meetings in the local research group, the two risk management workshops were discussed and assessed in terms of which actions were taken later by the two SPI teams. Present at the meetings were the four SPI practitioners, the three authors, and the fourth researcher. Both SPI teams found that the suggested framework provided a comprehensive overview of risk items and resolution actions. Many comments about the detailed lists of risk items and resolution actions led to subsequent modifications and rewording, but the aggregate structure that we had created based on the initial brainstorm and a study of the SPI literature was not changed.

The quality assurance improvement project was not very active during that period. The manager of the quality assurance project was not present at the risk analysis session and had not yet devoted full attention to quality assurance. The other project members were, therefore, mainly in a reactive mode, and little had happened. Risks surfaced during the analysis, but none of the practitioners were able to resolve these risks in practice. From this, we learned that realizing a risk and identifying a set of resolving actions do not ensure that actions are or will be taken. The practitioners that need to commit to the results of a risk analysis session should be present and involved in the session. After 7 months, there was no agreed-upon plan for the organizational implementation of quality assurance procedures. After 10 months, the quality assurance project had rolled out its procedures, but the identified risks

never were managed effectively and consequently impacted the initiative.

The project management improvement project, in contrast, had considerable activity. The main risk was that project managers would not find the improvement attractive and worth their effort. The strategy was, therefore, directed at creating incentives for the project managers. After 1 month, an appropriate incentive structure was in place. After 5 months, the project manager education was a huge success, and all project managers wanted to participate (Andersen, Arent et al., 2002).

Third Iteration

We started the third iteration by appreciating the lesson learned from the first two iterations: successful application of the risk management approach required participation of practitioners with sufficient authority to address key risks. By including these actors in the workshop, we ensure that they agree with the outcome of the workshop, and thereby increase the chances that the agreed-upon actions actually will be implemented. We also introduced a new way to document the process directly onto transparencies and paper versions of the templates.

In the third iteration, we tested the changes on a project that was responsible for establishing an organization-wide metrics program (Iversen & Mathiassen, 2003). The new documentation scheme made it easier for the participants to relate risk questions to their particular situation. We documented each risk in more detail by answering the following question: "What are the specific issues that make this risk particularly important?" As we progressed through the risk assessment, this made it easier to determine why something had been given a specific characterization. The session included a complete risk analysis. The practitioners found the identified actions useful and relevant, and they emphasized the benefit of having reached a shared, overall understanding of risks and actions. The practitioners suggested including the traditional distinction between consequences and probability of a risk into the process. To keep the approach as simple as possible, we decided not to implement this idea.

Fourth Iteration

For the fourth iteration, we made no changes, and applied the approach to an improvement project responsible for improving diffusion and adoption practices (Tryde et al., 2002). The session had three participants: two practitioners from Danske Bank's IT Department and the fourth action researcher involved in this project. All three found the approach generally useful. They found the analysis of the risk areas and the specific actions particularly useful, but they did not find summarizing the strategies particularly helpful. The participants emphasized the importance of not merely following the suggested lists of risk items and resolution actions, but also of supplementing this with a more open-minded exploration. "We haven't asked ourselves, 'what can go wrong?'" said one participant. They merely had considered each risk separately as it was presented to them.

Closing

We discussed and assessed the third and fourth risk analysis sessions with the four SPI practitioners and the fourth researcher at a later meeting of the local research group. The metrics program had suffered several setbacks due to political turmoil when previously hidden data about software projects' performance were publicized (Iversen & Mathiassen, 2003). Nevertheless, the risk analysis session led to actions that the project took later. The two main actions decided at the risk management session were: (1) develop and maintain top management's support and commitment and (2) create immediate results that are perceived useful by software projects. At a meeting 3 months later, it was reported that the project successfully

had convinced top management that the collected metrics results should be publicized in all of Danske Bank's IT Department, which later happened (Iversen & Mathiassen, 2003). The diffusion and adoption project was successful (Tryde et al., 2002). Many of the performed activities came out of the risk analysis. It was decided to exit the iterations at this point because the experiences from the four iterations suggested that the risk management approach was in a stable and useful form. Our final activity was eliciting lessons for the overall action research endeavor (Iversen et al., 2004).

Managing SPI Risks

This section outlines the resulting risk analysis approach. The method has been described in more detail in other published works (Iversen et al., 2002, 2004).

The approach to managing SPI risks is based on a framework that aggregates risk items into areas and risk resolution actions into strategies. The first part of the framework describes the relevant SPI risk areas; the second part outlines the potential SPI risk resolution strategies. The approach is intended to be applied to the risks faced by individual SPI action teams. Figure 1 illustrates the four different areas in which SPI action teams might identify risks:

- **The improvement area:** those parts of the software organization that are affected by the specific SPI initiative.
- **The improvement ideas:** the set of processes, tools, and techniques that the SPI initiative seeks to bring into use in the improvement area.
- **The improvement process:** the SPI initiative itself and the way in which it is organized, conducted, and managed.
- **The improvement actors:** those involved in carrying out the SPI initiative.

As an example, consider an SPI team concerned with introducing configuration management in software engineering projects. Here the *improvement area* includes the software development projects that will use configuration management and the people supporting the process after institutionalization. The *improvement ideas* include the configuration management principles relied upon by the SPI team and the tools and methods that are developed to support these principles. The *improvement process* is the improvement itself, the way it is organized, and the involved stakeholders. The *improvement actors* are the members of the SPI team.

The risk resolution actions that SPI teams can apply are aggregated into five different types of strategies, as shown in Table 4. The strategies are listed according to the degree of change we suggest the SPI team's risk-based intervention will cause. *Adjust Mission, Modify Strategy*, and *Reorganize* target the improvement project's orientation and organization; *Increase Knowledge* targets the involved actors' level of expertise and knowledge; and *Mobilize* targets alliances and energies that will increase the project's chance of success.

The mission of an SPI team on configuration management may be to introduce configuration management on all documents (including documentation, code, etc.) in all software engineering projects in the company. This mission could be *adjusted* to include fewer projects (perhaps only large projects, critical projects, or projects in a specific department) or to exclude certain types of documents. The SPI team's strategy might be to involve a few key developers to give input to the process and, based on this, select a standard configuration management tool that every project then has to use. *Modifying the strategy* may entail involving more (or fewer) developers or implementing the chosen tool gradually in each project. *Mobilizing* may involve establishing agreements with an existing method department, a production department, or other departments or persons that have a vested interest in the

results of the team's effort. The SPI team could *increase its knowledge* by attending courses on configuration management or SPI, or by hiring knowledgeable consultants. If the project is not organized optimally for the task at hand, the effort could be *reorganized*, e.g., by establishing a formal project, negotiating a project contract with management and the software engineering projects, or developing a new project plan.

To help SPI practitioners determine a strategy based on current risks facing the project, the approach offers a four-step process based on Davis (1982):

1. **Characterize Situation** by interpreting the profile and scope of the elements of Figure 1.
2. **Analyze Risks** to assess where the most serious risks are. This involves rating each of the detailed risk items in the risk lists for the four areas, and then determining which area carries the highest risk exposure.
3. **Prioritize Actions** to decide on a strategy that will deal effectively with the identified risks. Here, actors use a process that alternates between individual and group judgments to determine which strategy is the most sensible given the current assessment of risks facing the project.
4. **Take Action** by revising project plans to reflect resolution actions.

CONCLUSION

IT managers see risk management as a key to success (Barki et al., 1993). Such approaches help appreciate many aspects of a project: they emphasize potential causes of failure, they help identify possible actions, and they facilitate a shared perception of the project among its participants (Lyytinen et al., 1996, 1998). This indicates that organizations can benefit from adopting IT risk management to their particular needs. The method we have presented can be used for that purpose, and thereby adds to the portfolio of approaches that are available to adapt generic insights to specific organizations. Similar methods are, for example, available to tailor knowledge on software estimation to specific organizational contexts (Bailey & Basili, 1981).

The method builds on action research experiences that can help organizations address IT-related problems effectively in line with scientific insights. Our own experiences using the method indicate that a number of competencies are required to adopt the method effectively. First, we had intensive domain (SPI) and risk management knowledge. Second, we had general competence in modeling organizational phenomena that we used to identify and classify risk items and resolution actions. Third, we had experimental competence that we used to collect feedback from the test situations to iteratively arrive at the resulting approach. Each of these competencies is required to apply the proposed CPR method in other contexts. It is also important to stress that the method, like most action research processes, is a template that needs to be adapted and supplemented in action, depending on the conditions under which it is applied.

In addition to being useful in a specific organizational context, the CPR method can help tailor risk management approaches to new domains within information systems and software engineering, for example, business process innovation, integration of information services, and ERP implementation. Any form of organizational change enabled by IT is complex and difficult. Risk management, as illustrated well in relation to software development and SPI, is a highly effective way to bring relevant knowledge within a particular organization or domain into a form in which it can support and improve professional practices. We, therefore, encourage researchers and practitioners within information systems and software engineering to adopt action research to

tailor risk management to specific organizations and new domains.

We conclude this chapter with good advice to those who wish to create a risk management approach for their organization:

- Make sure practitioners are able to relate wording of risks and resolutions to their project.
- Be aware of whether the approach needs to be facilitated. For practitioners to apply the approach on their own, it must be simple or well documented and supplemented by training.
- Build in documentation of rationales along the way (what was it about a certain risk that made it particularly evident in this project?).
- Include mechanisms to ensure action. It is not enough to create a risk resolution plan — the project also needs to carry it out.
- Iterate until the approach is stable. Then keep updating risks and actions to stay current with changes in the context as well as in the literature.

REFERENCES

Alter, S., & Ginzberg, M. (1978). Managing uncertainty in mis implementation. *Sloan Management Review, 20*(1), 23-31.

Andersen, C. V., Arent, J., Bang, S., & Iversen, J. H. (2002). Project assessments. In L. Mathiassen, J. Pries-Heje, & O. Ngwenyama (Eds.), *Improving software organizations: From principles to practice* (pp. 167-184). Upper Saddle River, NJ: Addison-Wesley.

Andersen, C. V., Krath, F., Krukow, L., Mathiassen, L., & Pries-Heje, J. (2002). The grassroots effort. In L. Mathiassen, J. Pries-Heje, & O. Ngwenyama (Eds.), *Improving software organizations: From principles to practice* (pp. 83-98). Upper Saddle River, NJ: Addison-Wesley.

Bailey, W., & Basili, V. R. (1981, March 9-12). Meta-model for software development expenditures. *Proceedings of the 5th International Conference on Software Engineering*, San Diego, CA.

Barki, H., Rivard, S., & Talbot, J. (1993). Toward an assessment of software development risk. *Journal of Management Information Systems, 10*(2), 203-225.

Boehm, B. W. (1991). Software risk management: Principles and practices. *IEEE Software, 8*(1), 32-41.

Checkland, P. (1991). From framework through experience to learning: The essential nature of action research. In H.-E. Nissen, H. K. Klein, & R. A. Hirschheim (Eds.), *Information systems research: Contemporary approaches and emergent traditions* (pp. 397-403). North-Holland: Elsevier.

Chrissis, M. B., Konrad, M., & Shrum, S. (2003). *CMMI: Guidelines for process integration and product improvement*. Boston: Addison-Wesley Professional.

Davis, G. B. (1982). Strategies for information requirements determination. *IBM Systems Journal, 21*(1), 4-30.

Donaldson, S. E., & Siegel, S. G. (2001). *Successful software development*. Upper Saddle River, NJ: Prentice Hall.

Grady, R. B. (1997). *Successful software process improvement*. Upper Saddle River, NJ: Prentice Hall PTR.

Humphrey, W. S. (1989). *Managing the software process*. Pittsburgh, PA: Addison-Wesley.

Iversen, J., Johansen, J., Nielsen, P. A., & Pries-Heje, J. (1998, June 4-6). Combining quantitative and qualitative assessment methods in software

process improvement. *Proceedings of the European Conference on Information Systems (ECIS 98),* Aix-en-Provence, France.

Iversen, J. H., & Mathiassen, L. (2003). Cultivation and engineering of a software metrics program. *Information Systems Journal, 13*(1), 3-20.

Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2002). Risk management in process action teams. In L. Mathiassen, J. Pries-Heje, & O. Ngwenyama (Eds.), *Improving software organizations: From principles to practice* (pp. 273-286). Upper Saddle River, NJ: Addison-Wesley.

Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). Managing risks in software process improvement: An action research approach. *MIS Quarterly, 28*(3), 395-433.

Jones, C. (1994). *Assessment and control of software risks*. Upper Saddle River, NJ: Yourdon Press, Prentice Hall.

Keil, M., Cule, P. E., Lyytinen, K., & Schmidt, R. C. (1998). A framework for identifying software project risks. *Communications of the ACM, 41*(11), 76-83.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1996). A framework for software risk management. *Scandinavian Journal of Information Systems, 8*(1), 53-68.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1998). Attention shaping and software risk: A categorical analysis of four classical risk management approaches. *Information System Research, 9*(3), 233-255.

Mathiassen, L. (2002). Collaborative practice research. *Information Technology and People, 15*(4), 321-345.

Mathiassen, L., Munk-Madsen, A., Nielsen, P. A., & Stage, J. (2000). *Object-oriented analysis and design*. Aalborg, Denmark: Marko.

Mathiassen, L., Pries-Heje, J., & Ngwenyama, O. (Eds.). (2002). *Improving software organizations: From principles to practice*. Upper Saddle River, NJ: Addison-Wesley.

McFarlan, F. W. (1981). Portfolio approach to information systems. *Harvard Business Review, 59*(5), 142-150.

McFeeley, B. (1996). *Ideal: A user's guide for software process improvement* (Tech. Rep. No. CMU/SEI-96-HB-001). Pittsburgh, PA: Software Engineering Institute.

McKay, J., & Marshall, P. (2001). The dual imperatives of action research. *Information Technology and People, 14*(1), 46-59.

Moynihan, T. (1996). An inventory of personal constructs for information systems project risk researchers. *Journal of Information Technology, 11*, 359-371.

Ould, M. (1999). *Managing software quality and business risk*. Chichester, UK: Wiley.

Paulk, M. C., Weber, C. V., Garcia, S. M., & Chrissis, M. B. (1993). *The capability maturity model: Guidelines for improving the software process*. Upper Saddle River, NJ: Addison-Wesley.

Ropponen, J., & Lyytinen, K. (2000). Components of software development risk: How to address them? A project manager survey. *IEEE Transactions on Software Development, 26*(2), 98-112.

Schön, D. A. (1983). *The reflective practitioner. How professionals think in action*. New York: Basic Books.

Statz, J., Oxley, D., & O'Toole, P. (1997). Identifying and managing risks for software process improvement. *Crosstalk - The Journal of Defense Software Engineering, 10*(4), 13-18.

Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. *Administrative Science Quarterly, 23*, 582-603.

Tryde, S., Nielsen, A.-D., & Pries-Heje, J. (2002). Implementing SPI: An organizational approach. In L. Mathiassen, J. Pries-Heje, & O. Ngwenyama (Eds.), *Improving software organizations: From principles to practice* (pp. 257-271). Upper Saddle River, NJ: Addison-Wesley.

This work was previously published in Measuring Information Systems Delivery Quality, edited by E. W. Duggan and J. Reichgelt, pp. 244-264, copyright 2006 by IGI Publishing, formerly known as Idea Group Publishing (an imprint of IGI Global).