State of Software Risk Management Practice

Mira Kajko-Mattsson and Jaana Nyfjord

***Abstract*—Despite the fact that risk management has been with us for some time, little has been reported about its industrial status, its co-existence with the development models, and its compliance to standard risk management process models. In this paper, we explore the domain of risk management practice within 37 software organizations. We do this by first comparing the industrial status against a process model that is synthesized from a set of current standard risk management process models. We then investigate how the companies studied have integrated their risk management with software development. Regarding the state of industrial risk management practice, our results show that there are some discrepancies between the industrial practice and the standard models studied. The industrial organizations have not implemented all the important activities as prescribed by the standard models. The standard models, on the other hand, have failed to identify some of the important risk management phases and activities. Hence, this paper suggests a list of issues that need be addressed in both the standards and the industry. Regarding the integration practice, our results recognize that process integration in this domain is still in its infancy.**

***Index Terms*— process model, software development, process integration, agile methods.**

I. Introduction

For many years, risk management has been known within various traditional domains such as business, manufacturing, health care, warfare, sociology, and the like. It has been considered to be an enabler of risk-taking [7]. By identifying and controlling the risks, one may make better and more daring decisions when taking on complex challenging projects or when exploring new unknown grounds [7]. Recently, however, it has become recognized as a best practice in the software industry [4]. Reasons are many. Some of them are increased business volatility, constantly changing technologies, improved customer satisfaction, globalization, substantial impact on business disruption, and the like [29][37].

Much research has been conducted in the software risk management field in the past decades, for instance by [3] [6][7][22][23]. It has resulted in a number of frameworks and models suggesting risk types, risk management strategies, process models, and various performance measures [5][10][24][33][39]. Despite this, little is known about the state of practice within risk management. To the knowledge of the authors of this paper, there are no publications reporting on the status of the overall risk management process and on how it integrates with the development process. Hence, we dare claim that the software community currently lacks insight into the industrial state of risk management practice.

In this paper we investigate the status of the risk management process and its integration with software development in 37 software organizations. Our goals are: (1) to find out the status of risk management process in the industry today, (2) to evaluate standard process models against the industrial practice, (3) to find out how the industry has integrated risk management with their development processes, (4) to identify issues that might aid in improving the integrated process, and finally, (5) to find out the differences between agile and other development approaches.

The remainder of this paper is structured as follows. Section 2 describes the research method taken during our study. Section 3 describes a synthesized risk management model used in our evaluation work. Section 4 describes and motivates our evaluation criteria. Section 5 describes the status within the organizations studied. Finally, Sections 6 and 7 make concluding remarks and suggestions for future research.

II. Research Method

This section describes the research method taken during our study. Section II.A lists and describes the research steps. Section II.B describes the questionnaire used in our study. Finally, Section II.C discusses the sampling and validity.

A. Research Steps

During the first step, we studied a set of risk management process models. To achieve both breath and depth of the risk management domain, we chose publications of renowned industrial and academic institutions, including: (1) international and organizational standards, e.g. [12][30][38], (2) academic and industrial models, such as [1][5][6][30], and (3) various investigations made by individual researchers or researcher groups, e.g. [7][13][33].

The models studied vary somewhat with respect to some of the fundamentals of risk management as identified in [23][25]. In order not to miss anything, we have therefore synthesized a subset of these models into one common model. Our goal was to create as comprehensive a model as

Manuscript received October 22, 2008.

Mira Kajko-Mattsson is with the Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, Forum 100, SE-16440. Kista, Sweden. (E-mail: mira@dsv.su.se).

Jaana Nyfjord is with the Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, Forum 100, SE-16440. Kista, Sweden. (Phone: +46-8-162000; fax: +46-8-7039025; e-mail: jaana@dsv.su.se).

Table 1. The questionnaire used in this study

Section A – Introduction

1. What is you name?
2. What is your email?
3. What is your telephone number?
4. What is the name of your company?
5. What is the number of employees?
6. What is your role in the company?
7. What type of products/services does your company develop/provide?
8. What is generally the size of your projects?
9. What software development process model(s) do you use?

Section B – Risk Management

10. Does your organization identify risks?
11. What types of risks do you generally identify and manage?
12. Do you have a general process for managing risks?
13. Regarding the risk management process,
    a. Could you please briefly describe your risk management process and its phases (e.g. risk identification, risk analysis, monitoring and control and so forth).
    b. If you were to compare your current risk management process with the one we propose, what are the differences/similarities?
    c. Please, browse through the list of activities specified for each phase and identify which activities that you carry out in your organization.
    d. Does the figure below miss anything that you do for risk management in your organization?
14. What roles are involved in risk management?
15. If you have different types of risks, do you have models specialized to each risk type or do you just use your general model?
16. Do you follow any standard when establishing (defining and following) your risk management process?
17. Do you record (document) risk and risk management activities?
18. What exact risk information is recorded?
19. How do you record risk information? Please, describe briefly.
20. Does the recording of risk differ between phases of the software process? If yes, please describe the differences briefly.
21. Do you use any other ways to communicate risks in your software projects?
22. Do you have any risk management process owner?
23. Could I study the documentation describing your risk management process?
24. Are there any problems or shortcomings with your current risk management process? Please list and describe them.
25. Do you think that risk management is important?

Section C – Development and Risk Management Process Integration

26. Concerning the organizational levels (business and engineering), does your organization have the same levels?
27. Do you conduct risk management on the business planning level?
    a. Who conducts business (long-term) planning?
    b. Does7do this/these role/roles manage risks?
    c. How does/do this/these role/roles manage risks?
    d. What is the outcome of this phase?
    e. What are the main risk management activities in this phase?
28. Do you conduct risk management on the engineering planning level?
29. For each of the phases, (product roadmap, release and iteration planning)
    a. Do you conduct planning in this phase?
    b. Who conducts the planning in this phase?
    c. Does/do this/these role/roles manage risks?
    d. How does/do this/these role/roles manage risks?
    e. What is the outcome of this phase?
    f. What are the main risk management activities in this phase?
30. Do you conduct risk management in the implementation/development phase? Please, describe briefly.
31. Do you consider risks within testing? If yes, what types of risks do you encounter?
32. Is your risk management process integrated with the software development process model or is risk management treated as a separate process?
33. What criteria do you use for integrating the risk management process with the software process?
34. When integrating risk management with development process, what criteria should one use to achieve maximal results?
35. Are there any problems or shortcomings with how risk management is integrated in your software projects currently?
36. Could you please provide an example of a software project where risk management was a failure and a success, respectively? Please motivate briefly.
37. Do you think that integrating risk management with the software process is important?

Section D – Agile vs Traditional Software Risk Management

38. Can the risk management standards/templates presented in this interview be useful in agile environments?
39. Could we please quickly browse through the figures of the process and the risk information template and identify the parts that are pivotal in agile environment?
40. Is there any difference in how risk management is conducted in agile and traditional projects? Please, motivate briefly.

possible covering all the issues as suggested by the current risk management models. The synthesized model is based on [3][7][10][14]. It is described in Section III.

As a third step, we determined the comparison criteria to be used in our study. These criteria cover the fundamental aspects of risk management as identified in [25]. Using them, we then created a questionnaire whose questions were based on (1) these criteria, (2) the synthesized risk management process model [28], and (3) a template of risk management information [26]. The questionnaire is described in Section II.B and presented in Fig. 1.

In the fourth step, we used students to make the interviews. The students attended an advanced international software engineering course. In total, 37 interviews were conducted with representatives from 37 different software organizations. Finally, in the fifth step, we analyzed the answers and established a status within the companies.

B. Questionnaire

The questionnaire used in this study consisted of four parts. As can be seen it Table 1, in the first part, *"Section A – Introduction"*, we enquired about the background information concerning the interviewees and their organizations. In the second part, *"Section B – Risk Management"*, we investigated the state of risk management practice within the organizations studied. In the third part, *"Section C – Development and Risk Management Process Integration"*, we explored whether and how the organizations managed to integrate risk management with their development processes. Finally, in the fourth part, *"Agile versus Traditional Processes"*, we studied integration of risk management with agile methods. All these parts constitute a basis for our evaluation criteria, to be described in Section IV.

The questionnaire used in this study was open-ended and semi-structured. The purpose was to give freedom to respondents to answer in their own terms [40]. Such type of interviewing has a positive effect in a sense that while interviewing, one may elicit more knowledge about the studied domain. Its drawback however is the fact that the interviewer must possess a good understanding of the domain studied, in order to adequately react to irrelevant answers.

Due to the fact that we used students in our investigation, we run the risk that some answers might be misunderstood. To avoid misunderstanding, three preventive actions were taken. First, we presented our risk management model in detail to the students. Second, detailed directives regarding the expected answers, and possible follow-up questions were inserted into the questionnaire. The goal of the interview, the questions and the questionnaire design were also described and discussed in class together with the students. Third, the interviewees were asked to provide their names and contact details to allow the authors to contact them with follow-up questions.

C. Sampling and Validity

The data sampling method was convenience sampling [32]. This means that we did not control the choice of the organizations involved in our study. It was students who did it. Due to the fact that it was difficult to make organizations show willing for an interview, the students were allowed to

Figure 1. The six phases of our synthesized risk management model

choose just any organization (large/medium/small and/or private/ government) in any country. The only requirement was that the organizations studied should have a risk management process in place.

Many of our students, coming from an international master program in Sweden, chose organizations in their own countries. Hence, the countries represented in this report are China, Colombia, Denmark, Finland, Germany, Iran, Mexico, Morocco, Pakistan, Thailand, USA, Spain, and Sweden. Due to the sensitivity of the material presented herein, we do not name them. Some of them however are major well-known multinational organizations.

III. Synthesized Risk Management Process Model

This section describes our synthesized risk management process model. It consists of six phases: *Risk Identification (RI), Risk Analysis (RA), Risk Management Planning (RMP), Risk Monitoring and Control (RMC), Risk Sign-Off (RSO)* and *Risk Post-Mortem Analysis (RPMA).* The phases and their activities are presented in Figures 1 and 5, respectively, and briefly described in Sections III.A.1-6.

A. Risk Identification

During the *Risk Identification* phase, one makes an inventory of potential risks that may have impact on the achievement of the predetermined objectives [36]. As listed in Fig. 2, the phase starts with preparatory activities for the actual risk elicitation [30]. It continues with the actual risk elicitation using various techniques such as brainstorming, interviews, scenario analysis, prototyping, and the like [12][30]. When doing it, one identifies risks, their consequences, effects, sources, root causes, and categories [12]. Finally, one creates a risk list and circulates it around all the relevant stakeholders for possible complementary additions, improvements, and confirmation.

B. Risk Analysis

During the Risk Analysis phase, one analyzes and prioritizes risks [3]. First, one analyzes each risk independently by studying the identified risk and assessing its impact, probability, risk exposure and severity [36]. The analysis can be conducted using different techniques, e.g. matrices, decision trees and scenario analysis [30]. One then groups and analyzes the related risks to facilitate their collective mitigation [30]. Afterwards, one consolidates the risk prioritization and creates a top-priority risk list [3]. Based on the analysis results, one suggests a preliminary plan for managing each risk or risk group. Finally, the prioritized risk list is circulated among the stakeholders for confirmation.

C. Risk Management Planning

In the *Risk Management Planning* phase, one creates concrete plans determining strategies, options, and actions relevant for managing the identified risks [12]. As depicted in Fig. 5, one starts the phase with studying the risk list, the analysis results, and the preliminary plan [30]. For each risk or risk group, one first determines appropriate strategies [30], and then creates and documents the following three plans:

- *Control and Monitoring Plan* defining relevant measures or metrics for monitoring and controlling the risks [30],
- *Risk Action Plan* determining the actions to be used for treating a certain risk or risk group [36], and
- *Contingency Plan* specifying the actions to be taken in cases when severe risks turn into a serious problem [30].

One then combines all the three plans into one comprehensive *Risk Management Plan* [12]. To ensure that the identified risks get full attention, one prepares contractual agreements, where each risk owner's responsibilities are specified and agreed upon [30]. Finally, one circulates, updates and confirms the plan and its related documentation.

D. Risk Monitoring and Control

In the *Monitor and Control* phase, one continuously monitors and controls the risks according to the risk management plan. One also continuously identifies new risks. To make certain that risks are effectively monitored and controlled, one first ensures that there are risk monitoring procedures established. For each risk or risk group, one then continuously monitors and records the status [30]. In cases when the status changes, one takes measures as specified in the plan. Finally, one updates and records the risk status [12].

E. Risk Sign-Off

A formal sign-off phase is an important part of risk management assurance [36]. Here, one first reviews the risks and the way they have been mitigated. For each risk that is judged to be mitigated, one updates the risk management progress status, removes it from the risk list, and ensures that the risk list gets updated [36]. Finally, one signs it off.

F. Risk Post-Mortem Analysis

In the *Risk Post-Mortem Analysis* phase, one collects and evaluates the risk management process and its results. Here, one evaluates the information about the identified risks, their causes, treatment, the process used and the successes or failures of the actions taken. [12]. Using it, one then creates or updates the organizational risk taxonomy [30], if needed. Finally, one identifies successes and failures in the process and generates lessons learned [12]. This, in turn provides an important historical feedback for improving the future risk identification and management process [36].

IV. Evaluation Criteria

This section presents our evaluation criteria. Section IV.A lists and describes the criteria that were used when comparing our synthesized risk management process model with the industrial models. Section IV.B describes the criteria used for evaluating the industrial practice of integrating risk management with their software development processes.

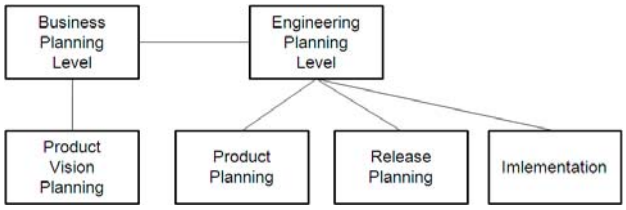

Fig. 2. Organizational levels and their phases

A. Criteria for Comparing Risk Management Process Models with the Industrial Practice

When studying the industrial status of risk management, we used nine criteria that covered some of the fundamental aspects of risk management [25]. Based on these criteria, we then created the first two groups of interview questions as listed in Table 1. The criteria and their related questions are briefly described below.

- *Risk identification practice*: Risk is an event or a condition that may affect the outcome of a project [12]. Its identification and classification is a prerequisite for effective risk management [12]. Questions 10 and 11 investigate whether and how the organizations studied identify and categorize risks.
- *Risk management process:* The risk management process consists of a set of phases and activities that are necessary for conducting risk management on software projects [30]. The phases generally consist of *Risk Identification*, *Risk Analysis*, *Risk Action Planning*, *Risk Monitoring and Control*, *Risk Sign-off* and *Post-Mortem Analysis* [12][14][30][38]. Using *Questions 12* and *13*, we investigate whether the organizations studied have a risk management process, and which phases and activities they perform. Using *Question 15*, we also investigate whether they tailor them to specific types of risks.
- *Roles and responsibilities:* Stakeholder roles are individual roles or role groups who have a stake in or may be impacted by a given activity [12]. The coverage of stakeholder roles within risk management is important. It is only then one may be sure that all the risk sources and targets have been identified and scrutinized from all possible perspectives. Designation of roles is a prerequisite for defining risk management process and responsibilities within the process [14]. *Questions 14* and *22* investigate what roles are covered by the organizations studied.
- *Use of models, standards and guidelines:* External risk management models and standards exist to provide critical guidance in defining a risk management process. Using *Question 16*, we examine which guidelines are used by the organizations studied.
- *Risk recording and documentation practice:* A clear, complete and correct risk description is an important prerequisite for its effective management [5]. To aid in maximizing the quality of the risk information, one should document the risk and provide guidelines for what information should be managed during the risk management process [11]. Using this criterion in *Questions 17*, *18* and *20*, we explore whether and what kind of risk management information is recorded. *Use of supporting tools*: To enable effective risk information management, analysis and tracking, organizations need tools and repositories for documenting the risks and risk management process [12]. Using *Questions 19* and *21*, we find out whether and what tools the organizations studied use for documenting risk management information.
- *Scope of risk management:* Risk management is recognized as best-practice in the software industry [4]. In current models, it is directed to software projects in general. However, we wish to investigate if there are any differences in their application depending on, for instance, the project characteristics. In order to identify the scope of applying risk management, we examine if risk management is applied in all types of projects in the organizations studied (*Question 26*).
- *Risk management process problems:* Problems related to the risk management process provide a good platform for evaluating the process, identifying its deficiencies, and for making process improvements. For this reason, using *Question 24*, we elicit risk management process problems within the organizations studied.
- *Importance of risk management:* Many voices have been heard regarding the importance of risk management [13]. These voices have mainly been raised within the academia. Little is however known about the attitude towards risk management within the industry. Hence, we find it out using *Question 25*.

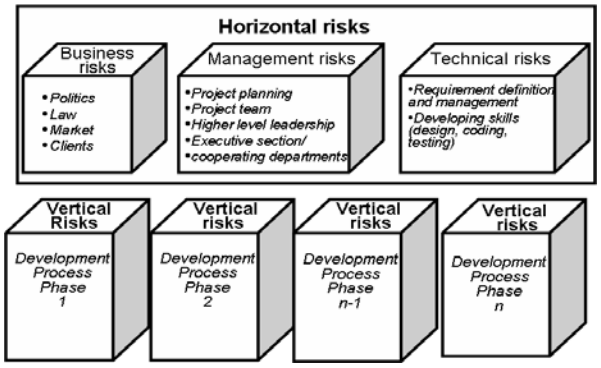

Fig. 3. One way of categorizing risks in *Organization 15*

B. Criteria for Evaluating the Industrial Practice of Integrating Risk Management with Software Development

To explore the industrial practice of integrating risk management with software development, we used the following five evaluation criteria:

- *Organizational levels*: Most software organizations conduct their business on various organizational levels [42]. As illustrated in Fig. 2, they usually distinguish between *Business* and *Engineering* levels [27]. The *Business* level involves planning of more strategic nature to establish the product vision, while the *Engineering* level involves realizing that vision by planning and developing the product [19]. Risk management is relevant for both *Business* and *Engineering* levels. For this reason, using *Questions 26-31*, we inquired about

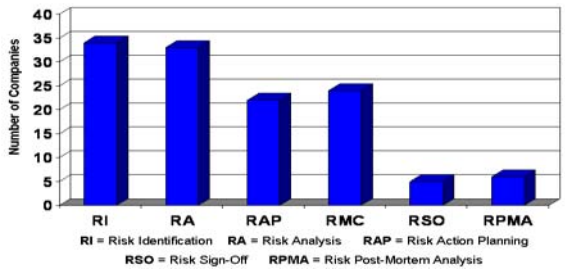

Fig. 4. Risk management process phases used in 34 organizations

the state of conducting risk management for each of these levels and their inherent process phases.

- *Integration aspects*: When integrating processes, one needs to identify appropriate criteria for doing it. Due to the fact that there are very few process integration models regarding this domain, we inquired about the criteria to be used when integrating risk management with software development. Hence, using *Questions 32 – 34*, we wished to find out (a) whether the organizations studied integrated their risk management processes with their development processes, and (b) the criteria they used in this integration.
- *Integration problems*: Problems, successes and failures provide a good platform for evaluating the integration attempts by indicating their deficiencies and strong sides.

  For this reason, in *Questions 35* and *36*, we elicited problems, successes and failures of process integration as experienced by the organizations studied.
- *Importance of process integration*: The software industry should have an opinion about the importance of integrating risk management with development processes. This opinion should be listened and paid heed to. It may provide indications of the procedures to be enforced or avoided during integration. To find them out, we asked *Question 37*.
- *Applicability of risk management in agile context*: Due to the fact that agile methods claim to be risk driven [2][8], we wished to hear the industrial point of view about this issue. For this reason, we first presented the synthesized process model (see Figures 2 and 5) and a template for managing risk information (see Fig. 6) in order to find out about their applicability in an agile context. We did it using *Questions 38-40*. We then inquired about the differences between the agile and other traditional development approaches with respect to the risk management practice.

V. Status

This section presents the risk management process status within the organizations studied. Section V.A describes the industrial risk management status whereas Section V.B describes their integration practice.

A. Risk Management State of Practice

In this section, we present the state of risk management practice within the 37 organizations studied. When doing it, we follow the order of the comparison criteria as listed in Section IV.A.

1) Risk Identification Practice

All the 37 organizations studied identify various risk types. The types identified include *Business*, *Financial*, *Project*, *Process*, *Planning*, *Resource*, *Technical*, *Organizational*, *Legal*, *Partner/Subcontractor*, *Country*, *Product* and *Quality* risks. Some organizations further classify risks into (1) *Internal* and *External*, and (2) *Horizontal* and *Vertical*. The *Internal* risks are risks that are encountered locally within the development organization whereas the *External* ones come from the external environment. The *Horizontal* risks spread across the whole software development cycle whereas *Vertical* risks only concern risks for a certain development phase. Fig. 3 illustrates the *Horizontal* and *Vertical* risks as managed in Organization 15.

2) Risk Management Process

Almost all of the studied organizations, 33 out of 37, have defined a risk management process model. The remaining four companies do not have any documented model. However, they conduct risk management in their respective companies. In one organization, it is claimed that their risk management process relies on tacit knowledge, whereas the other three organizations claim that their risk management is implicit in their agile development processes.

The interviewees were asked to compare their models with our synthesized risk management model and to point out similarities and differences. This has enabled us to establish their status and compliance with our model. As presented in Fig. 4, 34 organizations conduct the *Risk Identification* phase. Thirty-three out of 37 organizations conduct both *Risk Identification* and *Risk Analysis*. Twenty-two organizations have a *Risk Management Planning* phase, and 24 out of these 34 organizations also have *Risk Monitoring and Control*. Regarding the latter phases, *Risk Sign-Off* and *Post-Mortem Analysis*, only five out of 37 companies explicitly implement the *Risk Sign-Off* phase while only six implement the *Post-Mortem Analysis* phase.

The interviewees were also asked to study our model as presented in Figures 1 and 5 and point at the activities that they used within their own processes. The results provided by the 13 companies that responded to this question are presented with numerical values after the activity names in Fig. 5. Essentially, the results show that they only use some of the core activities of R*isk Identification, Risk Analysis, Risk Management Planning,* and *Risk Monitoring and Control.* However, all of the 37 interviewees claimed that our model was exhaustive, and that it did not miss any activities.

Eight out of 37 organizations have specialized their general process models for managing specific types of risks. The remaining 29 companies have not implemented any specialized models. They claim that (1) most of their risks are similar in nature; hence, their management is similar (2) it is too costly to develop and maintain several models, (3) it is unnecessary to create specialized models when there is a generic process model already, and (4) it is difficult to scope the specialization.

3) Roles and Responsibilities

The majority of the organizations studied put the *Project Manager* role in charge of risk management. His

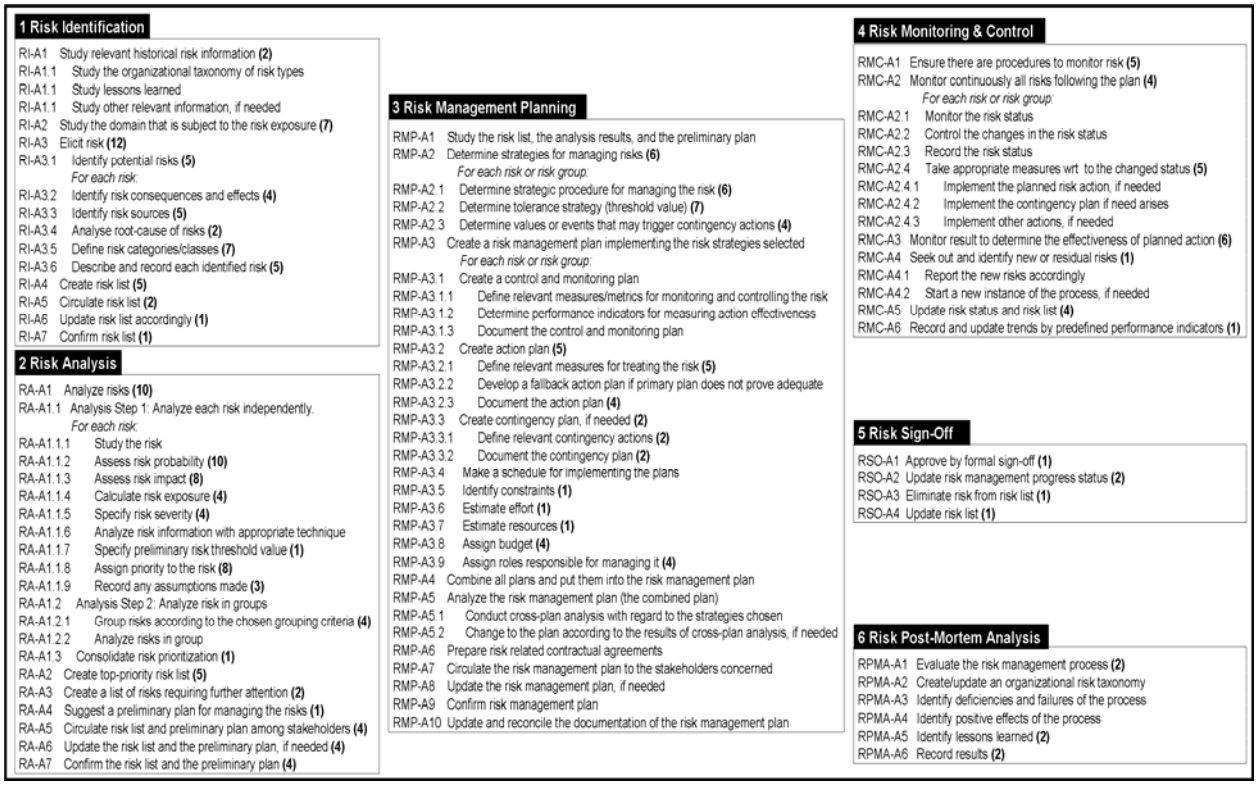

Fig. 5. Our synthesized risk management model, its phases and their activities

responsibilities are for instance, to organize the risk identification and analysis, plan and implement the risk mitigation plan, and to supervise the risk management process.

Our study also shows that in many companies, different roles are responsible for different risk types and their management. This distinction mainly depends on the process phase. We have identified the following roles:

- *Manager roles:* CEO, CIO, risk manager, risk management executor, project manager, team lead, release manager, various managers, e.g. product managers.
- *Analyst roles*: business analyst, requirements analyst, system analyst.
- *Boards/committees/departments:* senior executive committee quality and safety department, software engineering process group, project review group, supervision personnel.
- *Engineering roles/teams:* architect, developer, designer, quality engineer, tester, project team, development team, team members.
- *Other roles:* customer, chief scientist, expert, consultant, CM personnel, DBA, hardware staff.

4) Use of Models, Standards and Guidelines

Seventeen out of the 37 studied companies explicitly state that they follow a risk management standard, model or other official guideline. The standards, models or guidelines mentioned include the *CMMI (RSKM model)* [1], *Continuous Risk Management (CRM)* [37], *European Cooperation for Space Standardization (ECSS) standards* [9], *IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems* [16], *ISO/IEC Guide 73* [17], *ISO 9000* [18], *ISO 9001:2000* [19], *Caper Jones' model*[20], *Microsoft Solutions Framework (MSF) Risk Management Discipline* [21], *Open Unified Process (OpenUP)*[8], *PECAL/AQAP 160 Airborne Quality Systems* [35], *Project Management Body of Knowledge (PMBoK)* [30], *TL9000 Telecom Quality System* [31], *SAP Risk Management* [34], and *UNE EN 9100:2003 Aerospace Quality Management Systems* [15]. The remaining 20 companies have internal or organizational standards that they have developed on their own.

5) Risk Recording and Documentation Practice

All the companies studied communicate risks. All, but three, explicitly state that they record risks and risk management activities. Two of the remaining three companies use agile processes. They claim that there is no procedure for recording risks in these models.

The recorded information varies somewhat across the organizations studied. When being asked to study our risk template as presented in Fig. 6 and published in [26], only 26 companies were able to explicitly point at the data that they recorded. The results from these 26 companies are presented as numbers next to the attributes listed in Fig. 6.

Regarding the use of tool support for recording and communicating risks, all of the companies use some kind of a tool support dedicated for this purpose. The primary tools used include spreadsheets (23 companies), text editors (7 companies), internal tools (3 companies), whiteboard (2 companies), commercial project and risk management tools (1 company), and repository (1 company).

More than half of the organizations studied also use one or several complementary ways for communicating and recording risks. These are: meetings (20 companies), repositories (8 companies), brainstorming sessions (6

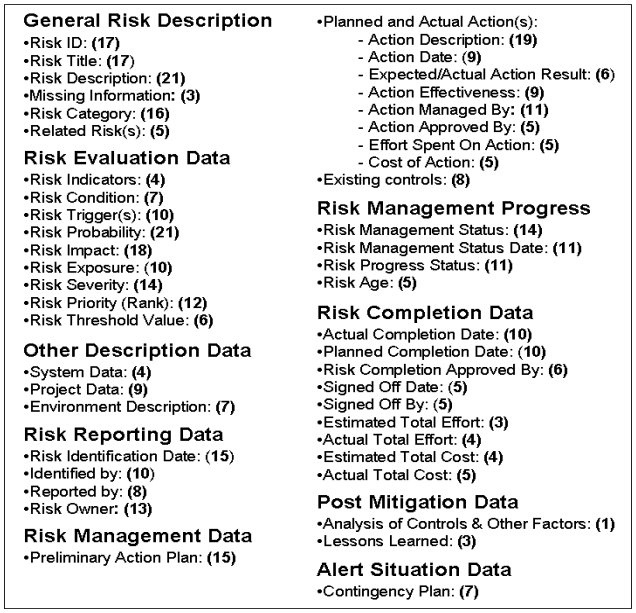

Fig. 6. Recorded risk information

companies), various forms of customer/team interaction (3 companies), email (2 companies), and informal discussions (2 companies). For instance, whiteboards are often used initially in brainstorming sessions, where risks are identified. The risks are later recorded in more formal documents.

In one of the agile organizations, risks are not recorded. The interviewee claims that there is no repository or procedure designated for recording risk information. In another agile company, spreadsheets are however used to document general project activities, and risks may be included in this documentation, if need arises.

6) Scope of Risk Management

Twenty-one companies lay a strong emphasis on risk management. Hence, they carry it out in all projects. In the other 16 companies, the use of risk management depends on several factors, i.e. project size, schedule, resources and degree of product innovation. One of the main reasons why risk management is not always applied concerns cost. For instance, in one of these organizations only projects over 100 person-hours perform risk management. The interviewees from these 16 companies are however of the opinion that all projects should use risk management; all projects have risks and it is important to attend to them.

Our results also show that the risk management process may be tailored according to a set of factors such as project size, schedule, and criticality. For instance, small projects consisting of 2-5 people do not need to apply risk management step by step. Regarding the agile companies, all adaptations are dealt with on an "on the fly" manner.

7) Problems with Risk Management

Eighteen out of 37 companies have experienced problems within risk management process. They are the following:

- *Attitude towards risk management process*: Many employees do not take risk management process seriously.
- *Scalability problem*: Informally defined risk management process models suit well for small projects. However, they are difficult to adapt to large projects.
- *Shortage of experienced risk managers*: The personnel do not possess satisfactory knowledge and experience within the risk management domain.
- *Lack of or insufficient tool/repository support:* Some organizations do not have tools for recording risk information or tools that provide enough feedback for making various analyses e.g., historical analyses.
- *Lack of process sophistication and completeness*: The industrial risk management process is too simple and/or incomplete. It does not cover all aspects of risk management.
- *Integration problems:* Risks are mainly considered in the context of software development. Other risks, such as environmental or organizational ones, are not always managed.
- *Lack of risk management process owner:* Some companies lack a role dedicated to risk management. Most of the responsibilities of the risk management process owner are managed by project managers, who, in turn, may not properly balance their responsibilities and priorities.
- *Lack of resources:* Organizations lack resources for performing risk management. Because of this, they may not be able to pay enough attention to identifying all risks and to fully monitor and control risks that may create serious problems.
- *Lack of process formality:* The organizations do not manage risks in a formal way. The process entirely relies on the experience of the individuals involved in it.
- *Terminology problem:* People have their own terminology which makes it difficult to communicate risks effectively.
- *Lack of process standardization:* The organizations have not defined a standard risk management process model. Hence, their risk management is very ineffective.
- *Lack of knowledge management:* There is neither a knowledge base nor a process for learning and spreading the knowledge about the risks and their impact.
- *Lack of formal and standard documents for recording information about risks:* Organizations do not have any guidelines for how to document information about risks. This in turn leads to non-uniform way of documenting risks, thus obstructing effective risk management.

8) Importance of Risk Management

All the companies agree that risk management is important. More than half of them claim that risk management is very important for the following reasons:

- The earlier you find the risk, the easier it is to mitigate it, thus leading to a lower total development cost.
- By controlling and mitigating the potential threat, one becomes preventive instead of reactive to various risks. In this way, one may avoid many serious problems in the future.
- A properly defined risk management process model is of great aid when prioritizing various types of risks, a task that is experienced to be very difficult by the organizations studied.

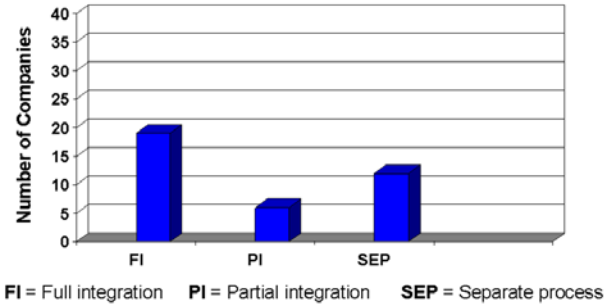

Fig. 7. State of process integration in 37 software organizations

B. State of the Integration Practice

This section presents the results regarding the state of practice of integrating risk management with development process. When describing them, we follow the order of the criteria as listed in our evaluation model in Section IV.B.

1) A. Organizational Levels

Thirty-two out of the 37 studied companies have the *Business* and *Engineering* levels (see Fig. 2). In the remaining five companies, the interviewees were not familiar with the work conducted on the *Business* level. Twenty-eight out of the 32 companies have a phase corresponding to the *Product Vision Planning* phase during which they manage risks. The risks managed at this stage are primarily business and market risks.

When managing risks in the *Product Vision Planning* phase, the organizations conduct their own risk management processes, mainly by having face-to-face meetings. The stakeholders involved in them are primarily represented by various senior management roles (e.g. *CEO, CIO,* and *CTO)* and the roles coming from the business department, such as sales and product managers.

Concerning risk management on the *Engineering* level, thirty-two companies claim that they conduct risk management using their own organizational risk management process models. They claim that the choice of activities, the types of outcomes and the roles involved vary depending on the engineering phase.

In the *Product Roadmap Planning* phase, the roles involved are mainly represented by various managers (business, product, project), customer, business analysts and requirements engineers. Since it is still a planning activity, the risk management activities conducted herein are *Risk Identification* and *Risk Analysis*. They are mainly conducted via meetings or brainstorming sessions.

Regarding risk management in the *Release Planning* phase, it follows the same organizational risk management process as in the previous phases. However, some differences were identified with respect to the roles and the risk management process phases. The roles identified in this phase include release managers, technical leaders, team leaders, senior software engineers and QA. The phases identified are *Risk Identification, Risk Analysis* and *Risk Management Planning.* There is also a shift in the focus on the types of risks managed in this phase. For instance, as stated by the interviewee of *Organization 21*: *"Risks in this phase concern issues such as the stakeholders' satisfaction with the release plan, and not only the business risks"*.

Regarding risk management in the *Iteration Planning* phase, fourteen companies state that they do not conduct *Iteration Planning* because they use non-iterative development approaches. In the remaining organizations, risk management in the *Iteration Planning* phase is conducted according to the organizational standards. The differences identified concern the roles involved, the risk management activities, and the types of risks focused on. The roles involved on this level are mainly engineers, represented by system architects, software engineers, testers, system integrators, and other roles. In a majority of the companies having iteration planning, risk management is led by the project manager. Generally, the activities in the *Iteration Planning* phase cover almost all the risk management phases, including *Risk Identification, Risk Analysis, Risk Management Planning, Risk Monitoring and Control* and *Post-Mortem Analysis.*

2) Integration Aspects

The integration of the software and risk management processes varies within the organizations studied. As illustrated in Fig. 7, nineteen companies have integrated their development processes with risk management, six companies have partially integrated them, and another twelve have them as separate processes. In the first group of organizations, risk management directly or indirectly affects the development activities, work products of the planning and execution process phases, and various parameters. It is an ongoing process that is carried out by the team throughout the whole project life cycle. In the next group of companies (six companies), the processes are claimed to be partly integrated. Reasons are varying. For instance:

- In *Organization 20*, one runs two separate processes, one for development and one for risk management. These processes have separate process owners. Although, these owners share the responsibility for managing and controlling risks, they still follow different processes for carrying out their work.
- In *Organization 4*, the degree of process integration depends on the project characteristics. In most of the projects, risk management and development processes are integrated. In large projects having complex risk profiles, one runs a separate risk management process. The reason is the fact that the risk management process requires more resources.

When integrating the processes, the 19 companies in the first group as identified in Fig. 7, mainly use criteria such as activities, resources and roles. They suggest that one

- assigns resources to the integration effort,
- adapts the integration process to the risk type by combining appropriate risk assessment and elimination techniques,
- identifies appropriate activities and resources for each risk type,
- adapts the risk management process to the project type, and finally,
- thoroughly documents information about risks and identifies development phases and activities that may be affected by the risk.

Several factors were pointed out to be important to achieve maximal results from process integration. These are:

- establish good communication between the development team and the risk manager (*Organizations 9* and *22*)
- involve the right people (*Organizations 26* and *31*)
- ensure that the people on the team have good collaboration skills (*Organizations 26* and *31*)
- determine which roles should do the risk management activities, and decide how they have to cooperate with the other roles (*Organizations 4* and *16*).
- assign the right risk management activities to the right development process phase (*Organization 16*).
- make the risk management process flexible to fit the development process model and the project needs (*Organization 3*)
- create risk integration architecture, i.e. a process integration model (*Organization 33*)
- continuously assess risk management and adapt the risk management process to the status at hand (*Organizations 5, 18, 23, 27, 34* and *37*)
- balance the processes with each other in order to avoid too much or too little focus on one or the other process *(Organization 8*)
- make the process homogenous. To achieve it, you have to make sure that the risk management and development activities belong to the same process and are treated in the same way (*Organization 13*)
- integrate risk management into the overall development plan (*Organizations 11* and *15*).

3) Integration Problems

Twelve out of the 37 organizations studied claim to have problems with the process integration. The problems identified are the following:

- Resource problems
  - Training cost is too high (*Organization 22*)
  - Lack of resources to conduct risk management (*Organizations 21* and *33*)
  - Lack of time to conduct risk management (*Organization 11*)
- Organizational problems (*Organization 16*)
  - Different roles have different attitudes towards risk and risk management (*Organization 29*)
  - Lack of competence (*Organizations 10*, *21* and *33*)
  - Work overload for project manager (*Organization 8*)
  - • Scope problems
  - Lack of control of external risks (*Organization 35*)
- Process problems
  - Lack of process coordination (*Organization 15*)
  - Lack of process integration (*Organizations 11*, *15* and *31*)
  - Lack of plan (*Organization 11*)
  - Lack of process (*Organization 31*)

One organization (*Organization 8*) points out that although integration is important, the success still depends on the project management. If the project manager can control the integrated process, it is an advantage. However, if the project manager has not enough time to have an overview of the whole process, a separate risk management process led by some other role can be more useful. The other twenty-five organizations claim that they have no problems at all. However, twelve out of them have not integrated their processes.

4) Importance of Process Integration

All the organizations claim that the integration of the software development and risk management processes is very important. They motivate this by stating that (a) applying a single process is easier than two different processes, (b) integration makes the risk management process much more effective, (c) risk management can help prevent problems, and (d) the organization will produce better software products with lower cost.

5) Applicability of Risk Management in Agile Context

The answers to the question regarding the usefulness and applicability of our synthesized risk management model (depicted in Figures 1 and 5) in agile environment vary between the organizations studied. They are the following:

- Sixteen companies state that the model is useful and applicable in agile environments. They claim that risk management is needed in any development model, whether traditional, agile or other.
- Eleven companies state that the model is partly applicable in agile environments. It threatens the balance of agility. Hence, it should be adapted to the agile context. *Organization 13* motivates this with the following: "*It goes into too deep details that can violate one of the basic concerns of agile environments, which is to keep software development process low-ceremony. Thus, some of the data need be refined to fit within the "simplicity" requirement of agile models*".
- Four companies claim that risk management is not useful in agile projects. They motivated it with the following: (1) the risk management model is too complex, (2) the agile model with its iterative approach already has risk management by its nature. Hence, the need for separate risk management is limited.
- Six companies did not respond to this question because they were not familiar with the agile process models. When being asked to go back to our model and to point out the phases that would be considered pivotal for agile projects, the following phases were pointed out: *Risk Identification* (17 companies), *Risk Analysis* (16 companies), *Risk Management Planning* (15 companies), *Risk Monitoring and Control* (15 companies), *Risk Sign-Off* (15 companies), *Risk Post-Mortem Analysis* (17 companies). Twenty-one out of 37 companies responded to this question explicitly. The remaining companies did not respond to this question because they felt that they were not sufficiently familiar with the agile models.

The results of *Question 25* indicate that the organizations studied are of the opinion that all the risk management process phases are relevant in an agile context. The organizations, however, had conflicting opinions about them. For instance, whereas 15 organizations identified the *Risk Sign-Off* phase as important, some voices were raised against it. The motivation was that the *Risk Sign-Off* phase would hurt the spirit within an agile team. Formal sign-offs would discourage the team members from collaborating with one

another.

Concerning the question about the differences between projects using agile and other types of process models, 16 out of 37 companies claim there are differences in how risk management is carried out in agile versus traditional projects. Five companies claim there are no differences and sixteen companies did not respond to this question. The differences identified are:

- *Time aspects:* The risk is not exposed until late in the traditional projects. The iterative nature of agile projects allow them to identify risk areas sooner rather than later (*Organizations 27, 31*, and *36*)
- *Development approach and risk management effort:* The iterative development approach minimizes risks and the total risk management effort (*Organizations 12* and *37*).
- *Follow-up and control mechanisms*: The risk management process activities are conducted sequentially in traditional approaches and usually managed via various documents and formal inspections, whereas risks are managed through other types of controls in agile models, e.g. via the backlog and daily meetings. The team continuously manages risks at the daily and other review meetings rather than via documents as in many traditional approaches (*Organization 14*).
- *Frequency of risk management*: In the agile context, risk management is conducted more frequently than in the traditional context. The agile cycle is shorter than in other models (*Organization 10*).
- *Level of process formality*: In agile environments, one usually does not have time for managing risks at the same level of detail that is described in traditional risk management models (*Organization 18*).

VI. Concluding remarks

In this paper, we have studied the industrial practice of risk management and its integration with software development in 37 software organizations. Regarding the industrial status of the risk management process, few organizations have implemented the entire process. The substantial majority of the organizations studied mainly apply the initial phases of *Risk Identification* and *Risk Analysis*. Despite this, they have provided us with an important feedback for identifying several shortcomings in the current risk management models. These shortcomings have helped us identify the following suggestions for improvements in the current risk management models:

- *Extend risk categorization:* The risk management models categorize their risks into *Internal* and *External* [30]. This is also the case in several of the organizations studied. However, we have also identified a new way of categorizing risks, not mentioned in any of the models studied. It concerns *Horizontal* and *Vertical* risks. In our opinion, it is a very important categorization showing that some risks may involve several processes and many different stakeholders at different organizational levels. It indicates that some risks are not amenable to one-dimensional classifications. For this reason, we suggest that the risk management models pay heed to this remark and revise the current risk categorizations.
- *Revise the set of risk management phases and activities:* Combined, the risk management process models studied prescribe a varying set of phases necessary for conducting risk management [12][30]. For instance, they may include or exclude the *Sign-Off* phase and the *Post-Mortem Analysis* phase. Our observations show that these phases are of great importance for the long-term effective risk management. For this reason, we dare claim that the individual models should address them to better match the industrial practice and needs.
- *Suggest appropriate process specializations:* None of the risk management models studied provide guidelines for how to tailor risk management process to specific project or organizational needs. Our observations show that not all of the activities in our model are applied in practice. The main reason is that the models are either too formal or general, and thereby, not always applicable in all situations. Our observations also show that there is a need for adapting certain parts of risk management process to specific types of risks and project needs. The specific risk types may concern for instance safety and security. Hence, we suggest that the models create appropriate process specializations to adapt to specific risk types and specific project needs.
- *Revise the risk management roles:* The models studied suggest a set of internal and external roles [12][30]. We have however observed that many more roles are involved. Hence, we recommend that the models re-assess their role portfolios and the risk management scope.
- *Re-assess the suggestions for the risk management information to be recorded:* The risk management models studied suggest that structured and disciplined communication is a prerequisite for the effective management of risks [11]. Our results show that the majority of the data recorded concern basic risk description and management data. Due to the fact however that we have not investigated the reasons for this in this study, we do not have any appropriate explanation. We can only suggest that similar studies be conducted to determine whether the standard guidance for recording risk management information should be revised.
- *Integrate risk management tools with the organizational tools:* The models studied suggest that one uses repositories for recording and storing risk information [12][23]. Our results show that the majority of the organizations studied do not use repositories. They mainly use simple tools, such as spreadsheets in combination with text editors and other. We believe that this is a serious omission and negligence in the organizations studied. Due to the fact that risk management process should be a driving wheel of the organization, its business and processes, it should be well integrated with other organizational processes so that one can easily react to changing situations. Hence, we suggest that the software community create a tool integrating risk management information with other organizational information.

- *Consider existing risk management problems:* Our study has revealed some problems within the industrial risk management processes. Problems vary and involve various aspects including processes, tools, people, dissemination, scalability, knowledge management, integration, resources, formality, standardization, and terminology. These problems constitute an important platform for analyzing and improving the current risk management models.

Regarding the integration practice, the majority of the organizations studied have fully or partially integrated their risk management with the software process. They mainly use criteria such as activities, resources and roles to realize the integration. However, the process integration is conducted on an ad hoc basis.

Our study has also revealed some problems within the industrial process integration. These problems primarily concern organizational issues, people, skills, processes, tools, resources, and knowledge management. These problems constitute an important platform for analyzing and improving the current process integration practice.

All the companies studied agree that the integration of risk management with software development is important. They claim that a properly integrated process is of great aid in managing risks effectively. To achieve successful process integration is however a task that is experienced to be very difficult by the organizations studied.

We have found that risk management is needed in any development model, whether traditional, agile or other. Although, there are claims that the agile models include risk management by nature, the agile models provide very general guidance for managing risks [25]. Risk management models, on the other hand, provide detailed guidance. In accordance with the majority of the organizations, we believe that agile models should be more active in integrating more risk management aspects. It is only in this way, one may make sure that risk management is implemented and run in an effective manner.

VII. Epilogue

The findings made in this study indicate that the standard models have not sufficiently reflected the practice and needs of the organizations studied. They also show that the industry studied has not implemented all the activities as prescribed by these models and that the integration of risk management with development is still in its infancy. The small sample size and the convenience sampling method should not allow us to generalize these findings. However, we believe that they provide a valuable feedback about the status of risk management process and about the exhaustiveness of the standard risk management process models studied. To confirm our results, we suggest that more similar studies be made.

VIII. References

[1] Ahern D., Clouse A., Turner R., *CMMI Distilled.* 2nd Ed. Addison-Wesley, Boston, MA, 2005.

[2] Beck K., *Extreme Programming Explained: Embrace Change*. 2nd Ed. Upper Sadle River, NJ, Addison-Wesley, 2004

[3] Boehm B., "Software Risk Management: Principles and Practices". IEEE Software, Vol. 8 (1), 1991, pp. 32-41.

[4] Brown N., "Industrial-Strength Management Strategies", IEEE Software, Vol. 13(4) , 1996, pp. 94-103.

[5] Carr M.J. et al., "Taxonomy-Based Risk Identification". SEI Technical Report CMU/SEI-93-TR-006 ESC-TR-93-183, SEI/CMU, Pittsburg, PA, 1993.

[6] Charette R., "Software Engineering Risk Analysis and Management", McGraw Hill, New York, NY, 1989.

[7] DeMarco T., "Risk Management for Software Projects". The Atlantic Systems Guild, Camden, ME, 2004.

[8] Eclipse Process Framework (EPF), *OpenUP Process*. URL: http://www.eclipse.org/epf/. Accessed November 2007.

[9] European Cooperation for Space Standardization (ECSS), *Space Project Management*. URL: http://www.ecss.nl/. Accessed November 2007.

[10] Fairley, R., "Risk Management for Software Projects". IEEE Software, Vol. 11 (3), 1994, pp. 57–67.

[11] Hulett D.T., "Key Characteristics of a Mature Risk Management Process". Proc. of the European Project Management Conf./PMI Europe, 2001.

[12] IEEE 1540, *IEEE 1540 Standard for Lifecycle Processes-Risk Management.* IEEE, New York, NY, 2001.

[13] IEEE Software, "Managing Risk" (special issue). IEEE Software, Vol. 14 (3), 1997.

[14] Institute of Risk Management, Association of Insurance and Risk Managers, National Forum for Risk Management in the Public Sector, *A Risk Management Standard.* IRM, UK, 2002.

[15] International Aerospace Quality Group (IAQG), *UNE:EN 9100:2003 Quality Management Systems-Aerospace-Requirements* (2003). URL: http://www.iaqg.sae.org/iaqg/publications/standards.htm. Accessed December 2007.

[16] International Electrotechnical Commission (IEC), *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*. IEC, Switzerland, 1998.

[17] International Standardisation Organzation (ISO), *ISO/IEC Guide 73 Risk management-Vocabulary-Guidelines for use in standards.* ISO, Switzerland, 2002.

[18] International Standardisation Organzation (ISO), *ISO 9000:2005 Quality management systems-Fundamentals and vocabulary*. ISO, Switzerland, 2005.

[19] International Standardisation Organzation (ISO), *ISO 9001:2000 for Quality management*. ISO, Switzerland, 2000.

[20] Jones C., Patterns of Software Systems Failure and Success. Boston, MA, International Thomson Computer Press, 1995.

[21] Microsoft, "Microsoft Solutions Framework-MSF Risk Management Discipline". URL: http://www.microsoft.com/technet//solutionaccelerators/msf/default.mspx. Accessed November 2007.

[22] Jones C., Patterns of Software Systems Failure and Success. Boston, MA, International Thomson Computer Press, 1995.

[23] Na K. et al., "Software Development Risk and Project Performance Measurement: Evidence in Korea." The Journal of Systems and Software, Vol. 80, 2007, pp. 596-605.

[24] Nidumolu, S., "The Effect of Coordination and Uncertainty on Software Project Performance: Residual Risk as an International variable". Information System Research Vol. 6(3), 1995, pp. 191-219.

[25] Nyfjord J. and Kajko-Mattsson M., "Commonalities in Risk Management and Agile Process Models". Proc. of 2nd Int. Conf. on Software Engineering Advances, France, 2007.

[26] Nyfjord J. and Kajko-Mattsson M., "Communicating Risk Information in Agile and Traditional Environments". Procedings of 33rd Euromicro Conference on Software Engineering and Advanced Applications, 2007.

[27] Nyfjord and Kajko-Mattsson, "Degree of Agility in Pre-Implementation Process Phases". Accepted at the 19th Australian Software Engineering Conference, Australia, March 2008.

[28] Nyfjord J. and Kajko-Mattsson M., "Software Risk Management: Practice Contra Standard Models". Technical Report, Department of Computer and Systems Sciences, Stockholm University/KTH, Sweden, 2008.

[29] Pearson N., "How Governance and Risk Management Enables Greater Innovation and Business Value from Information Technologies". URL: ftp://ftp.software.ibm.com/software/tivoli/presentation/GRM_UN_Presentation.pdf. Accessed November 2007.

[30] Project Management Institute, *A Guide to the Project Management Body of Knowledge* (PMBoK), 3rd Ed. ANSI/PMI 99-001-2004, PMI, Newton Square, PA, 2004.

[31] Quest Forum, *TL9000 Telecom Total Quality System*. Quest Forum. URL: http://www.tl9000.org/tl_all-docs.htm. Accessed November 2007.

[32] Robson C., *Real World Research*. Blackwell Publishing, 2002.

[33] Ropponen J. and Lyytinen K., "Components of Software Development Risk: How to Address Them? A Project Manager Survey". IEEE Transactions on Software Engineering, Vol. 26 (2), 2000, pp. 98-112.

[34] SAP, "SAP Solutions for Governance, Risk, and Compliance: SAP GRC Risk Management". URL: http://www.sap.com/solutions/grc/riskmanagement/index.epx. Accessed December 2007.

[35] Spanish Ministry of Defence (DGAM), "PECAL/AQAP-160 Airborne systems embedded SW developed by engineering organizations of EADS-CASA". URL:http://www.calidaddelsoftware.com/documentos/II%20Semana%20CMMI/03-%20EADS-CASA.pdf. Accessed November 2007.

[36] Standards Australia and New Zealand, *Australian/New Zealand Standard Risk Management AS/NZS 4360:2004*. 3rd Ed., Standards Australia/New Zealand, 2004.

[37] Software Engineering Institute/Carnegie Mellon University (CMU/SEI), "Risk Management". URL: http://www.sei.cmu.edu/risk/main.html. Accessed Nov 2007.

[38] Standards Australia and New Zealand, *Australian/New Zealand Standard Risk Management AS/NZS 4360:2004*. 3rd Ed., Stds Australia/New Zealand, 2004.

[39] Wallace L. and Keil M., "Software Project Risks and Their Effect on Outcomes. Communications of the ACM Vol. 47(4), 2004, pp. 68-73.

[40] Walker R., *Applied Qualitative Research*, Gower Publishing Company Ltd, 1985.

[41] Williams R. et al., "Software Risk Evaluation (SRE) Method Description (Version 2.0)". Technical Report CMU/SEI-99-TR-029, SEI/CMU, Pittsburg, PA, 1999.

[42] Zdravkovic J., *Process Integration for the Extended Enterprise*, Doctoral Thesis in Computer and Systems Sciences. Royal Institute of Technology, Sweden, 2007.