Commonalities in Risk Management and Agile Process Models

Jaana Nyfjord and Mira Kajko-Mattsson
Department of Computer and Systems Sciences
Stockholm University/Royal Institute of Technology
SE-164 40 Kista, Sweden
jaana@dsv.su.se  mira@dsv.su.se

Abstract

On the surface, agile and risk management process models seem to constitute two contrasting approaches. Risk management follows a heavyweight approach whereas agile process models oppose it. In this paper, we identify commonalities in these two process models. Our results show that they have much in common, and that a merge between them is possible.

1. Introduction

Merging risk management and agile process models sounds like mixing black and white and have difficulties to achieve proper shades of gray. At first glance, these two process models embody much contrast with respect to each other. Risk management assumes heavyweight detailed management whereas agile process models challenge it.

In this paper, we investigate and analyze agile processes from a risk management perspective to find their commonalities. Although these processes represent different approaches (engineering and management), we compare them due to the fact that agile models claim to be risk driven.

The remainder of this paper is as follows. Section 2 describes the methodology taken when conducting our study. Section 3 describes our comparison criteria and Section 4 analyses risk management models and agile process models using these criteria. Section 5 and 6 present conclusions and suggestions for future work.

2. Methodology

Our study is a literature survey of the state of art within risk management and its applicability to agile practices. It consisted of three phases: (1) Literature Collection and Study, (2) Creation of Comparison Criteria, and (3) Comparison

*To achieve both breath and depth of the risk management domain, we chose publications of renowned industrial and academic institutions, including: (1) international or organizational standards, e.g. [9][11][19][25], (2) academic and/or industrial models, such as [2][3][4][5][23][24][28], and (3) various investigations made by individual researchers or research groups, e.g. [8][10][12][16][20][27]. We then chose a subset of them for our final analysis. They are the IEEE 1540 Standard for Software Lifecycle Processes - Risk Management [9], the Project Management Body of Knowledge (PMBok)[19], and the Software Risk Evaluation Method (SRE)[28]. We did the same with agile processes. The agile subset includes eXtreme Programming (XP) [1], Lean Software Development [18], and Scrum [21].

In the first phase, we studied risk management in depth. This helped us identify fundamental aspects of risk management. These aspects constitute basic criteria for our comparison. We used them to create a roadmap in the Creation of Comparison Criteria phase. Finally, in the Comparison phase, we analyzed the risk management and agile process models using the roadmap criteria. This helped us to identify common parts in the two approaches studied, and also recognize future research challenges.

3. Comparison and evaluation criteria

When studying the models, we used the following comparison criteria: (1) Risk definition, (2) Templates,
3.1. Risk definition

Risk is an event or a condition that may affect the outcome of a project [9]. It is characterized with two distinctive elements: probability and impact [16]. The probability defines the likelihood that a risk event may occur. The impact defines the outcome of a risk. Risk can be either a loss or a gain (an opportunity). A loss is an unwanted or negative effect whereas a gain is positive or progressive effect. In this paper, we investigate whether and how the models studied define risk. A definition is a prerequisite for defining risk management process. It helps in understanding the process and facilitates the comparison process.

3.2. Templates

A clear, complete and correct risk description is an important prerequisite for its effective management [4][8][28]. To aid in maximizing the quality of the risk information, one should provide guidelines for what information should be managed during the risk management process [4]. Figure 2 illustrates such guidelines in form of a template. Using this template, we investigate whether the models studied provide suggestions for how to structure risk information. We also investigate the coverage of the information as managed by the models studied.

3.3. Repository and experience base

To enable effective risk information management, analysis and tracking, organizations need repositories (preferably electronic) for documenting risks and the risk management process [9]. They should also be able to extract important experience and lessons learned which they may in turn use in various contexts, such as process assessment, improvement, root cause analysis, resource assignment, and the like. For this, they need experience base recording historical risk information.

We investigate whether the models studied suggest use of repositories and experience bases for documenting risk management information.

### Figure 2. Risk management information

(3) Repository and experience base, (4) Stakeholders, (5) Risk assessment, (6) Lifecycle, (7) Environment, (8) Organization, (9) Measures, and (10) Product. They are illustrated in Figure 1 and briefly described below.

3.4. Stakeholders

Stakeholder roles are individual roles or groups of roles who have a stake in or may be impacted by a given activity [9]. Stakeholders can either be internal or external. Internal stakeholders include any managerial or technical roles participating in a project, including project managers, developers, testers, maintainers, product owners, business analysts and managers, quality managers and support personnel [19]. External stakeholders are other roles, such as customers, contractors, suppliers and sponsors [9].

The coverage of stakeholder roles within risk management is very 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 [11][19].

We investigate what stakeholder roles are covered by the models studied, and which of the roles are provided guidelines for managing risks.

3.5. Risk assessment

To make right and informed decisions, it is of importance to correctly identify and analyze risks. Hence, one needs to classify and assess them [24].

Risk taxonomies (classifications) help identify risks systematically and thereby facilitate the analysis process [28]. However, they do not suffice for an exhaustive risk analysis. They need be complemented with various assessment properties (attributes) such as Risk Probability, Risk Impact, Risk Priority, Risk Exposure, and the like [3]. Values should be assigned to these attributes. Due to the fact that risk assessment is subjective, it may be difficult to assign relevant values [24]. Hence, guidelines for assessing risks in form of various techniques should be provided.

Taxonomies, assessment attributes and techniques greatly help organizations in planning various measures such as designation of risk management, estimation of the mitigation effort size, and identification of policies to guide them. We examine if the models studied specify risk taxonomies. We also
Figure 3. Core processes of risk management

examine if they suggest attributes and techniques for assessing risks.

3.6. Lifecycle

Effort spent on mitigating risks within development may be wasted if one does not consider risks within the whole lifecycle process [9][19]. Risk management activities may differ in various lifecycle processes. We investigate whether the models studied cover risk management within the total lifecycle process, what lifecycle processes they approach and whether they provide guidelines for the particular processes.

3.7. Environment

To implement risk management effectively, the team should consider the project in its cultural, social, international, political and physical contexts [19]. Systems may be developed in distributed and non-distributed environments. In a non-distributed environment, the team(s) is(are) co-located and work(s) together. The environment is 100% non-distributed if the customer is internal.

Regarding the distributed environment, it can span from having to deal with only external customers to having to deal with distributed teams in different organizations and different countries, where aspects such as culture can play a crucial role for the effectiveness [7]. Hence, the degree of distribution and its associated risks should be considered in risk management. We investigate whether the models studied consider a distributed environment and if guidelines are provided for addressing various environmental matters.

3.8. Organization

To adopt a risk management program successfully, factors such as attitude towards risks, organizational maturity, competency and training should be considered [8]. It is harder to implement risk management effectively in immature and incompetent organizations or with risk averse attitude [8]. Hence, all the stakeholders involved should acquire proper training in the product they produce/acquire and the processes they use. We examine whether the models consider attitude, competence and maturity and provide guidelines for dealing with them.

3.9. Measures

One of the main purposes of risk management is to identify uncertainties and take actions to either remove or transform them into acceptable risks [29]. For this, one needs a portfolio of appropriate measures in place. Such a portfolio covers processes suggesting activities for attending to risks, resources required for performing the processes and policies for ensuring that procedures and strategies for conducting risk management are defined and agreed upon [9][19].

The middle box in Figure 3 outlines a risk management process as covered by most of the models today, e.g. by [9][11][19][25]. To provide useful feedback to the organization, the process needs to be integrated with other organizational processes such as various lifecycle and measurement processes and policy management. These processes should continuously provide feedback on risks, their progress, resources used, effectiveness of the resources and policies chosen, and plans for contingency readiness [27]. We investigate whether the models studied suggest risk management processes and whether they provide guidelines for resource management, process measurement, policy management, and integration with other processes.

3.10. Product

Instances of the risk management process vary strongly with respect to the quality of the product, its life expectancy, and life cycle stage [9]. For this reason, risk management models should consider the product aspects when managing risks. Risk management may vary greatly in aged systems whose quality is undermined, life expectancy is low, and the system is close to retirement. We investigate if the models studied consider product status related issues such as quality, life expectancy and lifecycle stage.

4. Evaluation

In this section, we compare and evaluate the risk management models and agile process models using the criteria as described in Section 3.
4.1 Risk definition

The risk management models studied commonly define risk as an adverse condition or event that will affect the project. In addition, the PMBoK model explicitly recognizes the positive impact of risk.

Regarding the agile definition of risk, it is similar to those provided by the risk management models. Risk is defined as anything that has not yet happened but may happen and may jeopardize the success of the project [6]. In addition, XP considers risk as opportunity [1].

4.2. Templates

Only two out of the risk models studied provide templates for how to structure the risk management information. They are the IEEE 1540 Standard and the SRE method. The SRE provides the most detailed template. This template is presented in form of a taxonomy-based questionnaire ensuring that all risk areas are systematically addressed [4]. The other risk models provide general structures to be adapted to the situation at hand. In terms of information coverage, only suggestions on a general level are listed, e.g. risk evaluation and action plans should be registered.

The agile models studied do not suggest any specific templates for describing risks. Nor do they provide guidelines for what risk information should be managed by the process.

4.3. Repository and experience base

All the risk management models studied suggest the creation and support of an electronic repository for documenting risks. They also suggest the registration of experiences gained when mitigating risks.

The agile models do not suggest repositories and experience bases for documenting risk management information. The informative workspace is used in favor of electronic repositories, i.e. big visible charts or story walls [1]. Process improvement and risk reassessment occurs continuously in the agile retrospective meetings [14], where risks or concerns are generally revisited as part of determining future changes [21][22]. Electronic repositories are prescribed, only if need arises.

4.4. Stakeholders

All the risk management models studied state that the process should support the perspectives of all relevant stakeholder roles, both of the internal and external ones. They however suggest different sets of stakeholder roles. For instance, acquirers are mentioned in IEEE 1540 standard only. Furthermore, the models only identify the roles having responsibilities towards mitigating risks. These roles are commonly referred to as risk owners. Out of them, guidelines for how to manage risks are restricted to the project manager role only.

The agile process models suggest teams as main stakeholder roles. The teams consist of (1) internal roles such as developers, testers, project managers, business analysts and (2) external roles such as customers. However, the agile models do not provide any specific guidelines for the designation of roles and responsibilities for managing risks. The team commonly owns the risk management process [22]. The agile project manager facilitates the process and makes the results visible.

4.5. Risk assessment

All the risk management models suggest that some structure be used to ensure a comprehensive and systematic process for identifying risks. They suggest use of various techniques, such as risk questionnaires, taxonomies, brainstorming, scenario analyses, lessons learned, and prototyping. However, only the SRE method provides a taxonomy of risks [28].

None of the agile models suggest any risk management taxonomies. Nor do they suggest any form of a systematic way of describing and classifying risks.

All the risk management process models studied suggest attributes for assessing risks based on probability, impact, severity, and priority. The values suggested by them are either on a nominal to ordinal scale. For instance, the PMBoK and the SRE method describe relative scales, where the values range from very unlikely to certain, or, low, moderate, high. Numerical scales suggested are either linear or non-linear.

All the risk management models also suggest various techniques for assessing risks, that is, for assigning values to these attributes. The granularity level of these suggestions varies strongly, ranging from very coarse-grained to detailed ones. For instance, the IEEE 1540 standard only states that different techniques should be used whereas the SRE method provides descriptions of how to calculate risk exposure. The techniques use numerical and/or relative scales, and they range from decision tree analyses, risk tables and matrices, to team member scoring and the like.
The agile models do not suggest any particular risk attribute values or any specific techniques for assessing them. The techniques they mainly suggest correspond to frequent team-based assessments where risks are qualitatively analyzed and re-analyzed [22]. Teams continuously inspect and evaluate risks in various meetings (release, iteration, and daily/hourly planning, retrospectives, reviews). They make a prioritized list of risks or concerns and assign values to them which they then post in the informative workspace [22]. Risks and the attribute values are generally displayed as different color notes indicating different priorities.

4.6. Lifecycle

The risk management processes studied support the software product lifecycle to a varying degree. For instance, the IEEE 1540 standard, claims that it provides support for risk management throughout the whole software lifecycle [9], both in the context of primary and supporting processes. In contrast, the SRE method only creates a baseline for initiating a risk management process and does not cover any of the lifecycle processes. The PMBoK is a guidebook for managing all kinds of projects and does not focus on processes related to software engineering. It focuses on managing risks within the frame of a project. This means that if it were applied in a software project, it would primarily cover the development phase.

The above-described results allow us to conclude that none of the models studied covers other lifecycle processes than development. Although they claim to cover the entire lifecycle, they only concentrate on development on a project level. Very little consideration is being made to other primary life cycle phases such as evolution, acquisition, and maintenance. No consideration is being made to supporting processes such as release management, front-end support, configuration management, and the like.

The iterative, incremental and evolutionary approach in agile processes means that in each iteration, enhancements, corrections and minor improvements are being made in parallel. Hence, the agile approach automatically covers most of the primary processes such as development, evolution and maintenance. Due to frequent meetings, we conclude that the agile processes seem to better cover most of the primary and supporting processes. However, they do not describe how their practices differ in them.

4.7. Environment

Except for the SRE method, the risk management models mention the environmental aspects and discuss their importance in implementing risk management. The models claim that cultural, social, international, political and physical contexts should be considered. However, none of them provides explicit guidance for how to deal with these aspects in practice. Instead, they refer to other models or complementary methods. When quickly reviewing these references, we found very few traces of managing risks from an environmental perspective. Neither did we find any suggestions for managing distributed and multicultural environments.

The agile models provide some guidelines for how to adapt projects with respect to environment. For instance, we interpret the XP principles of humanity, mutual benefit, diversity, failure, reflection, opportunity and improvement as some form of guidelines for teambuilding and addressing cultural issues [1]. Regarding the distribution, the agile models are most effective in smaller, co-located teams [17].

4.8. Organization

Regarding organizational issues, such as attitude, maturity, and competence, all the risk models studied agree that they should be actively overviewed. Although the models differ in focus and level of detail, they provide some guidelines for tackling organizational issues. These guidelines range from policies, agreements to various preventive actions. For instance, to prevent risk averse culture, the models suggest that organizations should effectively communicate risks. Education and training are also important tools for increasing risk management maturity and for decreasing risk averseness.

These guidelines are however relatively general in comparison to the ones provided by the agile process models. Many of the agile practices and principles are centered on how to organize projects and teams effectively with regard to maturity, attitude and competence. They include guidance on how to build relationships, create incentives for sharing knowledge, and promote active learning in software projects [1].

4.9. Measures

Risk management covers three core components: risk management processes, resources and policies. Regarding the processes, all risk management models, except for the SRE method, focusing on risk
identification and analysis only, define an entire risk management process model. They define most of the activities as outlined in Figure 3. They explicitly cover Risk Identification, Risk Analysis, Risk Planning, Risk Treatment, and Risk Monitoring and Control. The only difference lies in the fact that they use varying terminology. They implicitly cover the Post-Mortem Risk Analysis. None of them however, explicitly suggests a Sign-off phase.

Except for the SRE method, all the risk management standards and models suggest that risk management tightly collaborates with measurement processes for achieving effective monitoring and control. Regarding the lifecycle models, only the IEEE 1540 standard states that risk management should be integrated with other lifecycle processes.

None of the agile process models explicitly suggest risk management phases as outlined in Figure 3. The agile models are however integrated with measurement processes in their own specific way. They use empirical process control, implying that one continuously inspects the process using various techniques, such as for instance burn down charts [21]. Using these techniques, they evaluate different environmental, organizational and technical variables in software projects, such as time, quality, requirements, resources, tools and development techniques [15].

Regarding the risk management resources, all the risk management models studied provide guidelines for how to allocate resources to risk management. They mainly refer to human resources such as designations of roles and responsibilities. Regarding agile models, they express this issue rather vaguely. They state that all the resources required to ensure project effectiveness should be made available [1].

Considering the risk management policies, the agile process models do not specify risk management policies or strategies. On the other hand, all the risk management models suggest that policies for risk management process be defined. However, the models are very general and vague in their suggestions. They mainly suggest that policies and strategies be in place. The only issue that they are explicit about is contingency plans. They claim that contingency plans or mitigation plans should be developed for all risks above their thresholds values.

Only, the IEEE 1540 standard clearly states risk management policies and strategies. By policies, they mean organizational knowledge regarding the risk management, whereas by strategies, they mean plans or methods for implementing the policies.

### 4.10. Product

Only the SRE process model describes risks and risk management with regard to the product status. It helps identify risks that can affect the delivery and quality of the product. However, it does not relate product status to specific risk management measures. Product related risk sources are specified and categorized in the SEI risk taxonomy [4]. Product status is not discussed in any of the other risk management models.

Considering agile process models, they do not provide any guidelines for relating product status to risk management. Product status related issues such as quality, life expectancy entirely rely on the priorities set by the customer and the team.

### 5. Conclusions

In this paper, we have compared current risk management and agile process models in order to identify their commonalities. We did it using a roadmap covering fundamental aspects of risk management. Although these models represent different approaches (engineering and management), we compare them due to the fact that agile models claim to be risk driven. We have found that the agile models studied make some assertions about risk management. However, they do not provide any detailed suggestions for managing risks, thus leaving many areas unattended. In summary, our conclusions and suggestions are the following:

- The definition of risk is the same in risk management and agile models. However, the recognition of risk as an opportunity is not as explicit in risk management as in agile models. We believe that both positive and negative effects of a risk should be considered in any risk management activity. It is only then one will be able to identify opportunities for progress and properly evaluate the effectiveness of risk management [19].
- Neither the majority of risk management nor agile models suggest templates for communicating information about risks and their management, despite the fact that high risk information quality is one of the most important prerequisites for effective risk mitigation [8]. In our opinion, both risk management and agile process models should be complemented with guidance for what information to collect and how to structure it.
- Risk management and agile models differ in the way risk information is recorded. Generally, risk management models advocate permanent storage
whereas agile models advocate temporary one. Risk management models suggest a risk management repository and experience base, supported by electronic tools. The agile models, on the other hand, mainly use the informative workspace. From a risk management perspective, permanent recording of risk information is the only way of assuring that all important information is being remembered, paid heed to and that lessons learned can be easily disseminated to enable process improvement [9]. In this respect, we suggest that agile methods should consider the idea of permanent storage as a complement.

- Both the risk management and agile approaches suggest some guidance for their stakeholder roles, mainly project managers. However, none of them suggest guidance for all other roles that might be relevant in the risk management process. In our opinion, both approaches should identify and recognize other stakeholders, such as maintainers, support personnel, to ensure that all the risk sources and targets have been identified and scrutinized from all possible perspectives.
- Risk management models provide support for classifying and assessing risks in form of taxonomies and various assessment attributes. Agile models do not do it at all. The assessment they generally suggest is designation of priorities via different coloring techniques. Risk management methods are aimed at mitigating risks and thus provide well established techniques for doing this. In this respect, agile models can learn from risk management models to ensure effective risk management.
- None of the risk management models studied encompasses management of risks within other lifecycle processes than development. Agile models cover development, enhancements and problem resolution in one and the same iteration, and to some extent other primary and supporting processes. We believe that both approaches should consider other lifecycle processes.
- None of the agile models explicitly suggest risk management phases. However, they implicitly cover them in methods like Scrum and eXtreme Programming. Risk management models, on the other hand, are better in explicitly suggesting risk management process phases. Despite this, they do not cover the Post-Mortem Analysis and Sign-Off phases. We believe that this is a serious omission. These phases are pivotal for making sure that serious risks have been attended to. Lack of this aspect leads to serious legal consequences.
- The risk management models studied suggest integration of risk management with measurement processes. However, they do not suggest any metrics or measurement models specific for risk management. Agile models integrate measurement processes. They use empirical process control, implying that one continuously inspects the process. Hence, our conclusion is that agile models seem to be better integrated with measurement models. We believe that the risk management models should provide suggestions for further enhancements of and integration with measurement models.
- Resource management is a prerequisite for effective operation in all models studied. Their allocation may differ with respect to risk management phase, risk severity, priority, and the like. Despite this, neither risk management nor agile models provide clear guidelines for how to manage resources. We suggest that the models studied complement their models with suggestions for how to allocate resources in various risk management phases and situations.
- The risk management models studied clearly state importance and functions of policies. However, they are vague about their contents. It is difficult to provide organizational wisdom in form of policies and strategies for implementing them. However, due to the fact that risk management should communicate collective knowledge and experience, we believe that they should provide some examples and motivations of policies and strategies. It is only in this way they may help organizations identify ways to carry out their missions and understand their implications.
- None of the risk management models studied provide guidelines regarding the environmental aspects of risk management. They refer to other models instead. Agile models, on the other hand, provide more practical guidance here. However, they do not consider distributed environments. We suggest that risk management models should learn from agile practices. In addition, we believe that both approaches should consider the distributed environment. Agile models have spread to distributed environments [26], but more evidence is needed from a risk management perspective.
- The risk management models studied herein provide only general guidance for managing organizational issues such as attitudes, training, and maturity. Agile models, on the other hand, provide relatively detailed guidance on how to deal with teambuilding, training and competence development. We believe that risk management models should be more active in recognizing the importance of these organizational issues. It is only in this way, one may make sure that it is implemented and run in an effective way.
• None of the models studied relates product status to specific risk management measures. This is an important factor to consider when tailoring risk management process to specific product status and allocating resources to it.

6. Epilogue

In this paper, we have found that the risk management and agile models studied have many parts in common. Although theoretical, our analysis shows evidence that there are openings for integrating them.

The conclusions presented herein can only be attributed to the models studied. We have not studied many other important models such as for instance RUP [13]. Hence, we cannot generalize our results. We may only suggest that similar studies be conducted using other models.

7. References