CS-TR-3782
UMIACS-TR-97-38

The Riskit Method for Software Risk Management, version 1.00

Jyrki Kontio

Institute for Advanced Computer Studies and
Department of Computer Science
University of Maryland
A.V. Williams Building
College Park, MD 20742, U.S.A.
Emails: jkontio@cs.umd.edu
jyrki.kontio@cs.hut.fi

Version 1.00
Status: Final

Abstract:

This paper presents the Riskit method for software engineering risk management. This document contains the motivation for the method, description of the Riskit analysis graph and a detailed description of the Riskit process.

Table of Contents

List of Figures

List of Tables

1. Introduction

This paper presents the Riskit method for software engineering risk management. The main features of the method are its sound theoretical foundations and its focus on qualitative understanding of risks before their possible quantification. Furthermore, the Riskit method provides a defined process for conducting risk management. The method is supported by various techniques and guidelines and the use of Riskit does not preclude the use of other risk management approaches.

The Riskit method has been integrated into the Experience Factory framework [3,7,8]. However, the experience capture aspect of the method is not addressed in this report, readers interested in that aspect of the method are kindly asked to refer to other publications [29-31] or contact the author for more information or for more recent publications.

An earlier version of the Riskit method has been empirically evaluated in a limited number of case studies [19,30,31]. This current version of the method (version 1.00) has been improved based on the feedback received from several case studies or evaluations carried out in industry and government organizations.

This paper is organized as follows. Chapter 3 presents key terminology in one place, although all terms are introduced as they are used in the paper. Chapter 4 presents the motivation for developing the Riskit method and explains its underlying principles. In chapter 5 we introduce the Riskit analysis graph. Chapter 6 presents the Riskit process in detail. Chapter 7 presents summary and conclusions and discusses further development plans as well as validation issues.

2. Acknowledgments

This work was initiated when I was working at Nokia Research Center. Pertti Lounamaa thus gave me the initial opportunity to lay the groundwork and build up the knowledge that made the development of Riskit possible. Professor Victor R. Basili at University of Maryland has had the most influence in this work. During my "research sabbatical" in Maryland we had frequent interactions and he had a strong impact on not only on this work but on many other areas that I have been working on. I am grateful for his support, encouragement and guidance in developing this method.

Olli Pitkänen of Helsinki University of Technology has made his expertise and insights available and reviewed earlier versions of this paper. His detailed and thorough feedback helped correct many errors and omissions. Gerhard Getto of Daimler-Benz AG has been equally important in providing feedback to the method. Especially his experiences from having used the method in practice resulted in many improvements that made the method more practical. Dr. Carylon Seaman's review of this report removed many ambiguities and improved internal consistency of this document.

I am grateful for all the help and contributions these individuals volunteered to this work. While I wrote this report, many advances in this report are the result of teamwork from the above individuals.

3. Terminology

We are using the following specific terms in this document:

- The term *risk* in its general meaning is defined as a possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility.
- *Risk element* is defined as any item in the Riskit analysis graph (see section 5 for details):
  - *Risk factor* is a known fact or characteristic that influences some risk event.
  - *Risk event* is an occurrence of an incident with some negative consequences.
  - *Risk outcome* is the resulting situation after the risk event but before any reactions have taken place.
  - *Reaction* is a (set of) corrective action(s) that are taken after the risk has occurred.
  - *Risk effect* is the combined impact of risk event and resulting reactions to goals of the project.
  - *Utility loss* is the harm a stakeholder experiences on a set of risk effects in a situation.
- *Risk scenario* is a combination of risk elements that describe the causes, triggering events and the impact of a risk. Normally a scenario consists of a risk event, risk reaction and risk effect set.
- *Riskit analysis graph* is a graphical formalism used to document risk scenarios in the Riskit method.
- *Risk item* is defined as a risk that has not been analyzed and categorized into risk elements or described in the Riskit analysis graph.
- *Risk cluster* is a grouping of risk items.
- *Risk controlling action* is a proactive maneuver that is taken before risk occurs (or before it is known whether the risk has occurred).
- *Stakeholder* is a person or organization that has an interest in the project or its results.
- *Goal* is defined as a characteristic that the project or product should have. Goals in the Riskit method are categorized into objectives, drivers and constraints (see section 6.2, page 19).

When an item has been used and defined for the first time in the text, it has been written in *italics*.

4. Motivation for Risk Management

Software development is often plagued with unanticipated problems which cause projects to miss deadlines, exceed budgets, or deliver less than satisfactory products. While these problems cannot be eliminated totally, some of them can be controlled better by taking appropriate preventive action. Risk management is an area of project management that deals with these threats before they occur. Organizations may be able to avoid a large number of problems if they use systematic risk management procedures and techniques early in projects.

Several risk management approaches have been introduced during the past decade [11,13,14,25] and while some organizations, especially in the U.S. defense sector [11,18], have defined their own risk management approaches, most organizations do not manage their risks explicitly and systematically [38]. Risk management based on intuition and individual initiative alone is seldom effective and rarely consistent.

When risk management methods are used, they are often simplistic and users have little confidence in the results of their risk analysis results. We believe that the following factors contribute to the low usage of risk management methods in practice:

- Risk is an abstract and fuzzy concept and users lack the necessary tools to define risk more accurately for deeper analysis.
- Many current risk management methods are based on quantification of risks for analysis and users are rarely able to provide accurate enough estimates for probability and loss for the analysis results to be reliable. On the other hand, the table based approaches are often biased and too coarse for risk prioritization.
- Risks have different implications to different stakeholders. Few existing methods provide support for dealing with these different stakeholders and their expectations.
- Each risk may affect a project in more than one way. Most existing risk management approaches focus on cost, schedule or quality risks, yet their combinations or even other characteristics (such as future maintenance effort or company reputation) may be important factors that influence the real decision making process.
- Many current risk management methods are perceived as complex or too costly to use. A risk management method should be easy to use and require a limited amount of time to produce results, otherwise it will not be used.

Given the increasing interest in risk management in the industry, we believe that for risk management methods to be applied more widely, they will need to address the above issues. Furthermore, risk management methods should also provide comprehensive support for risk management in projects, they should provide practical guidelines for application, they should support communications between participants, and they should be credible.

The Riskit method was developed to address the issues listed above. Its main characteristics can be described by the following principles.

(1) The Riskit method provides precise and unambiguous definitions for risks.

The common definition of risks, either by dictionaries or every day usage, associate several different meanings to risk. It can refer to a possibility of loss [1], the actual loss that would result if the risk occurs [1], a factor or element that is associated with a threat [1], or a person that contributes to the possibility of loss [2]. The dictionary definitions for risk are so broad that it is fair to define risk as anything that is related to the possibility of loss. Clearly,

there is some value in having such a broad and encompassing concept to facilitate initial discussion about risk. However, we believe that this wide range of meanings associated to the word ‟isk”can also prevent adequate precision in more detailed analysis or risks unless this ambiguity is explicitly addressed and removed.

The Riskit method contains means to define risks more precisely and formally. When we use the term risk on its own, we are using it in its general meaning: risk is defined as *a possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility*. As in most risk management approaches, we consider probability and loss the two main attributes of risk. However, our approach explicitly recognizes that the definition of loss depends on expectations, which in turn depend on stakeholders of the project. A loss is defined as an outcome that falls short of what was expected. As different stakeholders value outcomes differently, stakeholders influence the definition of loss in a project. This view is visualized in Figure 1.

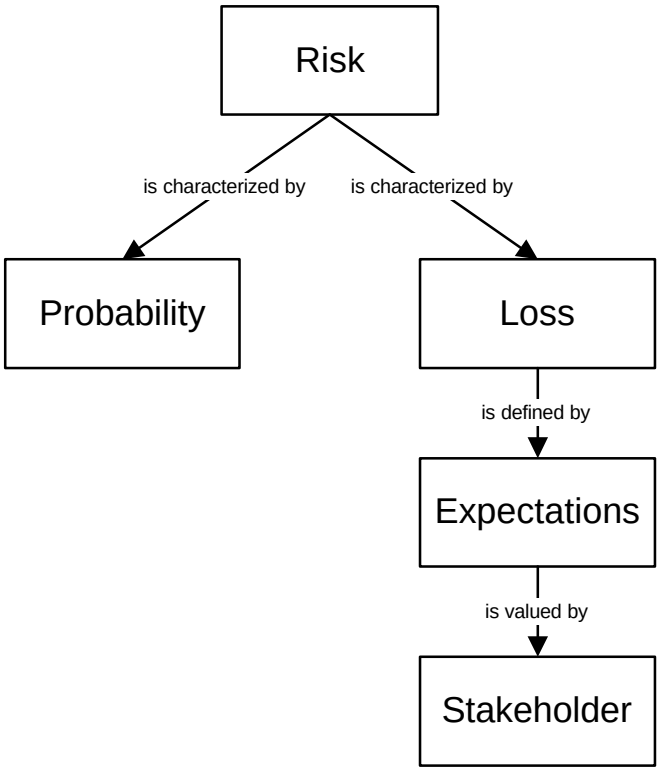


Figure 1: Definition of risk in the Riskit method

(2) The Riskit method results in explicit definition of objectives, constraints and other drivers that influence the project.

As we pointed out in Figure 1, risk is a relative concept; its definition depends on expectations that are associated with a situation. In order to analyze risks, it is necessary to formalize the expectations as well as possible. When expectations are recognized and defined, we refer to them as *goals*. While some goals cannot be stated precisely, at least they should be identified and documented as well as the information available allows. The Riskit method contains an explicit step and supporting templates to assist in the goal definition.

(3) The Riskit method is aimed at modeling and documenting risks qualitatively.

The Riskit method provides conceptual and graphical tools to model different aspects of risks qualitatively, instead of requiring quantitative estimation of risk probability and impact to take place early in the project. Given the difficulty of these estimations –and the often ambiguous interpretations of risks –the margins of error in risk quantification are easily high. By emphasizing the qualitative understanding of risks, there is a better basis for understanding and communicating about risk.

(4) The Riskit method can use both ratio and ordinal scale risk ranking information to prioritize risks reliably.

The estimation problem has been reduced in the Riskit approach. Instead of forcing the quantification of risks using ratio scale metrics –often an unrealistic goal –the Riskit method only attempts to accomplish the necessary quantification of risks for risk management to take place. For risk management purposes it may be enough to identify the biggest risks and propose action to control them, while the exact values of probability and loss may not be needed. The selection of the type of metrics to be used in risk analysis should be based on the objectives of the analysis and the availability of data about risks.

(5) The Riskit method uses the concept of utility loss to rank the loss associated with risk.

Many current risk management approaches are based ranking of risks based on the loss they cause to some specific attributes of the project, such as cost, time delay, or quality metrics. Often a single metric is used. This can be detrimental for two reasons. First, the use of a single metric, or a small number of metrics, can create strong bias away from secondary, yet influential goals that should be considered. Second, research in economics and management science has strongly indicated that decision are made based on the changes in the expected utility (or utility loss) of alternatives. As the utility functions of stakeholders are likely to be non-linear, use of direct loss metrics can lead to wrong estimates and rankings of the risks. Therefore, the Riskit method uses the concept of utility loss to compare and rank losses of risks.

(6) Different stakeholder perspectives are explicitly modeled in the Riskit method.

All projects have more than one stakeholder that is interested in its results. They may have different priorities and levels of expectations. Risk management should be based on the recognition of these stakeholder expectations and priorities. Traditional, direct project metric based approaches cannot easily support the comparison of different stakeholder views and few risk management approaches attempt to address the issue. The Riskit method supports stakeholder views by documenting their expectations explicitly and evaluating the utility loss for each separately.

(7) The Riskit method has an operational definition and training support.

The Riskit method has an operational definition so that it can be applied easily and consistently. This, in fact, is the main contribution of this paper, this paper presents an operational definition of the Riskit process. There is also a Riskit tutorial available and an application guideline paper is being written.

We suggest that by adhering to the principles described above the Riskit method is a comprehensive, operational, theoretically sound and practical method for software risk management.

5. Decomposing Risk: The Riskit Analysis Graph

The *Riskit analysis graph* is a graphical formalism that is used to define the different aspects of risk more formally. The Riskit analysis graph can be seen both as a conceptual template for defining risks, as well as a well-defined graphical modeling formalism. In both cases, it can be used as a communication tool during risk management. The Riskit analysis graph has been developed based on the ideas presented by Rowe [27,39], but we have evolved Rowe's notion of risk estimation steps into a well-defined, extended graphical formalism. In the following we will introduce the Riskit analysis graph first by a conceptual definition of its underlying elements, then by an operational definition of the graphical formalism that is used in practice to represent the underlying, conceptual model.

The underlying conceptual model – or meta-model – of the Riskit Analysis Graph components is presented in Figure 2, using the UML notation [37]. This meta-model represents the underlying, conceptual elements and their relationships. Each rectangle in the graph represents a risk element and each arrow describes the possible relationship between risk elements. The relationship arrow is read in the direction of the arrow. For example, the relationship between "risk factor" and "risk event" in Figure 2 should be read as *"[a] risk factor influences [the] probability of [a] risk event."*

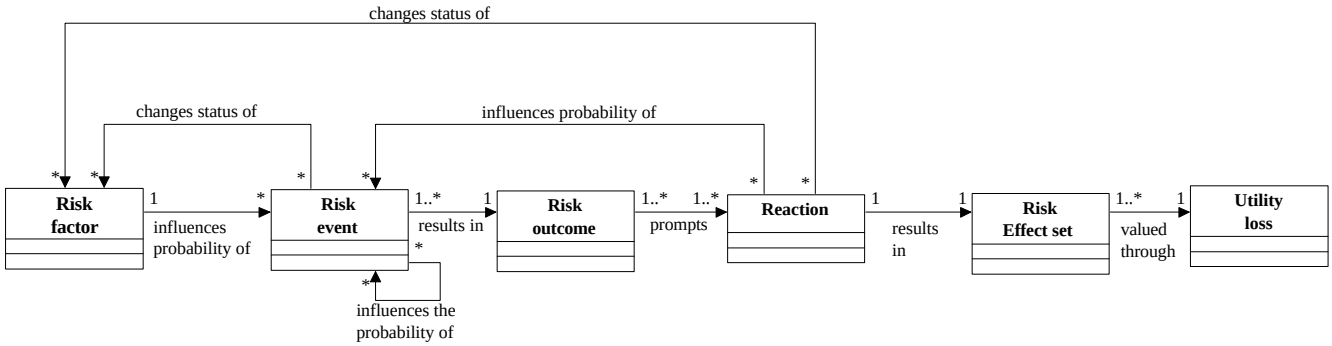


Figure 2: A conceptual view of the elements in the Riskit analysis graph

A risk factor is a characteristic that affects the probability of a negative event (i.e., risk event) occurring. A risk factor describes the characteristics of an environment. Consequently, in the Riskit analysis graph a risk factor does not have probability associated with it, it describes a relevant environment characteristic as it is or will be[1]. Examples of risk factors are listed in Table 1. Risk factors that are documented typically increase the probability of risks events occurring, but they may also reduce them, i.e., they are *success factors* for a project (e.g., "the development team recently developed a similar application").

[1] In practice it is possible that some risk factors are probabilistic, i.e., it is not known whether they are true for the environment or not. For instance, if new people are recruited for a project, it may be possible that a factor called "inexperienced personnel" becomes true. Such a situation is modeled by defining a risk event that influences a risk factor, i.e., risk event would be called "recruiting results in inexperienced personnel" and it would have a relationship to a factor called "inexperienced personnel."

Risk element	Software Engineering Examples	General Examples
Risk factor	• inexperience of personnel • use of new methods • use of new tools • unstable requirements[2]	• a high cholesterol diet • living near a fault line of earth's plates (e.g., San Francisco) • slippery driving conditions (rain, snow)
Risk event	• a system crashes • a key person quits • extra time spent on learning a method • a major requirements change	• a doctor's diagnosis of a patients heart problem • an earthquake • a car accident
Risk outcome	• system out of operation • personnel and competence shortage • work behind schedule • new work required	• a diagnosed heart disease exists • some buildings and roads destroyed • a crash scene: untreated personal injuries, damaged vehicles
Risk reaction	• system operational after delay, back up data restored • recruiting process initiated, staff reassigned	• treatment of heart problem • reconstruction of roads and building • treatment of injuries, purchase new car
Risk effect	• added cost $50K • two-month calendar delay • some functionality lost • reputation as a reliable vendor damaged	• hospital stay, cost of medical care • cost and inconvenience of reconstruction, loss of human life, medical expenses • medical costs, permanent injury effects, raised insurance premiums
Utility loss	• The perceived harm experienced by a stakeholder, e.g., the board of directors, CEO, or personnel	• The net effect of pain, lost time and expenses as felt by individuals

Table 1: Examples of risk elements

The purpose of risk factors is not to document all possible characteristics that may influence a risk event as there may be an infinite number of such factors. Instead, a risk factor should document main assumptions of project environment and, especially, characteristics that are different from the assumed, "normal" situation. This interpretation of risk factors enables explicit documentation of main assumptions and deviations from these assumptions.

A *risk event* represents an occurrence of a negative incident – or a discovery of information that reveals negative circumstances. Risk event is a stochastic phenomenon, i.e., it is not known for certain whether it will happen or not. This uncertainty can be characterized by a probability estimate associated to the risk event. Examples of risk events are listed in Table 1. Each risk event can be influenced by many risk factors but a risk event does not have to have a risk factor associated with it. A risk event can also influence the probabilities of other events or even influence risk factors.

The next element in Figure 2 is called *risk outcome*. It represents the situation in a project after the risk event has occurred but before any corrective action is taken to reduce the effects of a risk event. Examples of outcomes are listed in Table 1. The purpose of the concept of risk outcome is to document the immediate results and situation after the risk occurs. Based on the risk outcome description, different reactions can sometimes be considered more objectively and creatively than directly from a risk event.

When a risk event occurs, the resulting risk outcome is rarely accepted as such. Instead, organizations react to the situation to reduce the negative impact of the risk event. These

[2] Note that this is different from "a change in requirements," which would be a risk event. When defined as a factor, "unstable requirements" refers to the characteristics of the situation.

corrective reactions[3] are an important part of understanding what is the overall impact of the risk event to the project domain. Thus, each risk outcome is associated with one or more risk reactions: a *risk reaction* describes a possible action that can be taken as a response to risk event and resulting risk outcome. If only one risk reaction is described, it is deterministic: it will be taken if the event occurs. If more than one reaction is described, they represent alternative lines of actions. Risk reactions can influence the probabilities of risk events. If the influence is stochastic, they have a similar relationship as a risk factor has to a risk event: they change the probability of an event. Examples of risk reactions are also listed in Table 1.

The *risk effect set* represents the final impact of a risk event to the project. In other words, it documents what characteristics of the project were effected, taking into account the impact of reactions. Effects are described through the explicitly stated goals for the project. Examples of different effects on goals are listed in Table 1.

While the risk effect represents the impact the risk had on each project goal, the concept of *utility loss* captures how severe the overall impact of effects is. The concept of utility loss is based on the utility theory[4], a concept widely used in economics and decision theory [23,45]. The use of utility theory allows the simultaneous consideration of multiple criteria and consideration of several stakeholders. Furthermore, it is likely to result in more realistic evaluation of the losses as the utility functions of stakeholders are generally believed to be non-linear [10,24] and there may be points of discontinuity in them. We have sometimes used the term "pain" as a synonym for utility loss as the concept of utility may appear too theoretical for practitioners.

The multiplicity (i.e., cardinality) information about risk element associations is included in Figure 2, using the UML class diagram notation and syntax[5]. A symbol in the beginning of an arrow indicates how many outgoing associations are allowed or required. Correspondingly, a symbol at the end of the association arrow indicates how many associations can be linked to an element.

The Riskit analysis graph uses specific symbols to represent risk elements. The allowed symbols in the Riskit analysis graph are defined in Table 2. The banners of the symbols are color-coded to support easier recognition of risk elements[6]. The Riskit symbols can be drawn manually or with any drawing tool. However, we have implemented a drawing template on a MS-Windows -based drawing tool [44] which contains the Riskit symbols and thus supports easy creation and editing of Riskit analysis graphs.

[3] Note that we use the term "reaction" to action that is taken after the risk event occurs, as opposed to "risk controlling actions" that are taken before risk events occur.

[4] The utility theory states that people make relative comparisons between alternatives based on the utility (or utility loss) that they cause. The utility is the level of satisfaction, pleasure or joy that a person feels or expects.

[5] The multiplicity symbols are interpreted as follows:

1	Exactly one association leaves or enters the class.
*	Any number of associations leave or enter the class
1..*	At least one association leaves or enters the class.

[6] The color of the symbol is mentioned in parenthesis in the explanation column in Table 2 so that colors are distinguishable even when this document is viewed on black and white media.

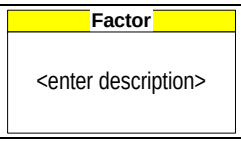
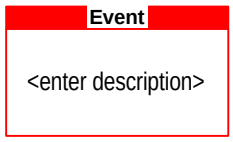
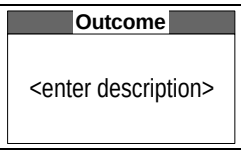
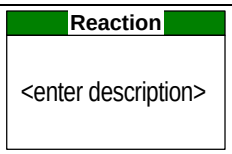
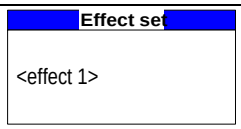
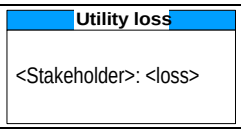
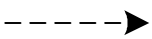
Symbol	Definition
	**Risk factor** (yellow banner). Represents risk factors. Risk factors name is entered in the symbol. The factor should be named so that its influence is unambiguous, e.g., one should name a factor "**limited** CASE experience" instead of just "CASE experience".
	**Risk event** (red banner). Represents risk events. Event name is entered in the symbol and the probability estimate of the event can be entered in the symbol as well.
	**Outcome** (gray banner). Represents the situation after the risk event has occurred but before reactions are carried out. Can be omitted.
	**Reaction** (green banner). Represents the actions that may be taken after the risk event has occurred. Descriptive name of the reaction entered in the symbol. The reaction symbol can be omitted from the graph for null reactions (i.e., when the reaction is "no reaction").
	**Effect set** (blue banner). Effect of a risk scenario to the situation. Each effect is described or quantified w.r.t. explicitly stated project goals. The effect is described as a deviation from the expected effect. If a goal is not effected, it is not listed.
	**Utility loss** (light blue banner). Documents the utility losses for each stakeholder. Can be omitted from the graph.
	Deterministic connector. Represents a certain relationship between risk elements in the Riskit analysis graph.
	**Stochastic connector**. The causality between risk elements is either probabilistic or is based on a decision to be made later.

Table 2: Riskit analysis graph symbols

Each class of symbols in the Riskit analysis graph is drawn in the same vertical column in a graph. In other words, if several risk scenarios are represented in the same graph, all factors are in the same vertical line (column), followed by risk events in the same column, etc. An exception is a case where some risk events only influence risk factors, i.e., they have been created to model probabilistic risk factors. These risk events can be placed towards left of the risk factor column to keep the main part of risk scenario more legible.

The utility loss is estimated for each relevant stakeholder. Thus, each risk effect set has at least one utility loss estimate associated with it.

The previous definitions introduced individual risk elements in the Riskit analysis graph: the term is used *risk element* to refer to any of the components presented above, i.e., risk factor, risk event, risk outcome, risk reaction, risk effect and utility loss (pain). We use the term *risk scenario* for any unique event-outcome-reaction-effect combination. Risk scenario is marked in Figure 2 with a dashed rectangle. The key attributes of a risk scenario are its probability, its set of risk effects and, its set of utility losses.

There are several possible ways to use the Riskit analysis graph. The *full Riskit analysis graph* is based on the underlying conceptual model of risk elements, as presented earlier in this section in Figure 2. However, our earlier evaluations with the method indicated that such a complete graph may be laborious to edit and complex to view in practice [31]. Therefore, a

simpler version of the graph can normally be used. In this normal version of the Riskit analysis graph the risk outcome is not explicitly modeled, it is implicitly included in the risk event, as is shown in Figure 3. This is called the *normal Riskit analysis graph* and it is the default version of the graph. The consequence of this simplification is that when there are more than one possible outcome for a risk event, these should be modeled as separate events.

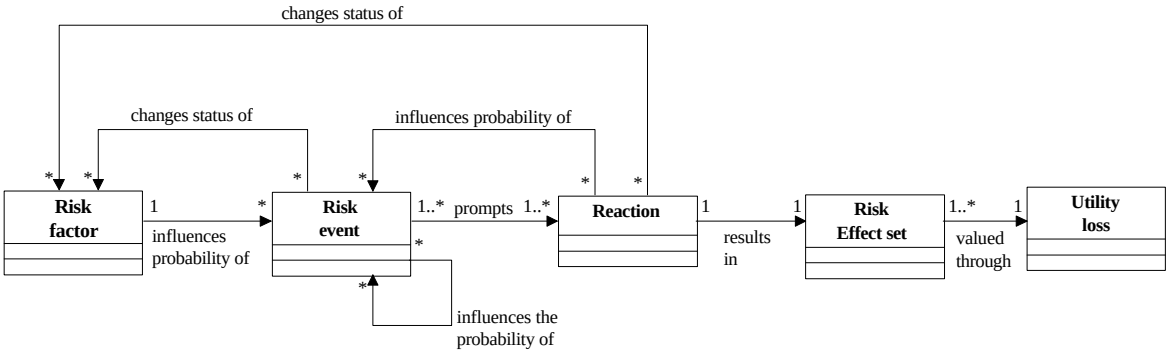


Figure 3: The "normal Riskit analysis graph"

We have also defined an even simpler version of the Riskit Analysis Graph, as shown in Figure 4. In this simplified form of the graph, the reaction element is implicitly included in the effect set element. This further simplification of the graph can be used when there is no need to model and analyze different alternative reactions and when there are reasons to minimize graph size and complexity. In a situation where the simple Riskit analysis graph is used and several reactions need to be modeled, they could be modeled as different effect sets. However, it is important to point out that the simple Riskit analysis graph makes a potentially central aspect of risk scenarios implicit. Thus, if alternative reactions need to be considered, we recommend that the reactions are explicitly modeled.

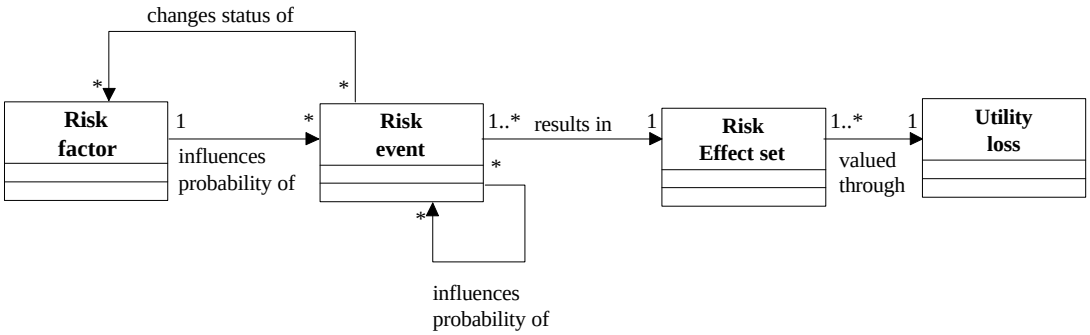


Figure 4: The "simple Riskit analysis graph"

6. Risk Management Process

In this section we present the Riskit risk management process. The Riskit process has been divided into distinct steps that are similar to other, widely used steps in risk management [12-14,20,33,39]. Our risk management process contributes to the previously presented ones by providing a process that is a "defined process", i.e., a process that is defined in detail so that it can be repeated consistently.

The Riskit process definition described in this document represents the risk management activities of the Riskit framework. The learning process included in the overall Riskit framework is based on the Experience Factory concept [3,5] and has been presented separately [29].

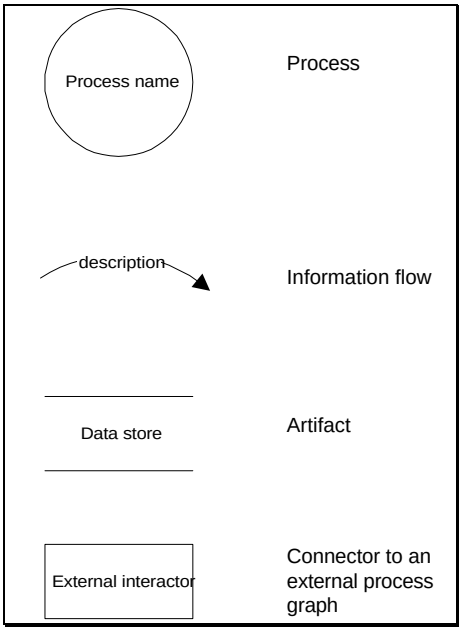


Figure 5: Dataflow diagram symbols used

The Riskit process definition includes the definition of items for each sub-process, as presented in Table 3. We have also represented the Riskit process graphically using the dataflow diagram notation [9,46]. The symbols used in the dataflow diagram notation have been presented in Figure 5. Note that the process symbol can also represent sub-processes.

Purpose:	Purpose of the process.
Description:	Description of the process and approaches used in it.
Entry criteria	The criteria that is used to initiate the process. The criteria can include logical expressions, such "AND" or "OR". The logical expressions area used, statements are written within square brackets: "[statement]".
Input:	Input information required by the process.
Output:	Output produced by the process.
Methods and tools:	Methods and tools used by the process.
Responsibility:	A person or role that is responsible for the process.
Resources:	List of resource types that are used or participate in the process.
Exit criteria:	Exit criteria used to determine whether the process has been concluded. The criteria can include logical expressions, such as "AND" or "OR".

Table 3: Process definition information template

Using the template introduced in Table 3, we have given a process definition for the whole Riskit process in Table 4.

Purpose:	Provide project and organization management with accurate and timely information of the risks in a project. Define and implement cost efficient actions to control risks.
Description:	Monitor and manage risks continuously in a project.
Entry criteria	Project planning has been initiated.
Input:	Project authorization information: goals, resources, schedule, budget. Context and history information about the organization and its process.
Output:	Continually updated information about risks. Defined and implemented risk controlling actions. Experience and data about risks and risk management process.
Methods and tools:	The Riskit process definition. Riskit documentation templates. Riskit analysis graph definition and drawing tools. Risk identification checklists. Multiple criteria decision making tools. Word-processing and spreadsheet software.
Responsibility:	Project manager.
Resources:	Technical personnel. Stakeholder representatives.
Exit criteria:	Project has been completed or terminated.

Table 4: Process definition information for the whole Riskit process

While Table 4 presented a holistic view of the Riskit process, the following sections present a more detailed view of the Riskit process, i.e., its sub-processes, artifacts used, information flows, resources used, and its behavior. The risk management cycle in a project can be viewed as consisting of some basic activities: defining the scope and focus of risk management; review and definition of goals; risk identification and monitoring; risk analysis; risk control planning; and controlling of risks. Main flows of information between these processes are represented in Figure 6. Each of the processes in Figure 6 can be instantiated several times during the project duration and they may be enacted concurrently. This behavioral aspect of the process is modeled through the entry and exit criteria defined for each process [17,28,36]. However, typically the most critical instances of the risk management cycle are the ones enacted in the beginning of the project.

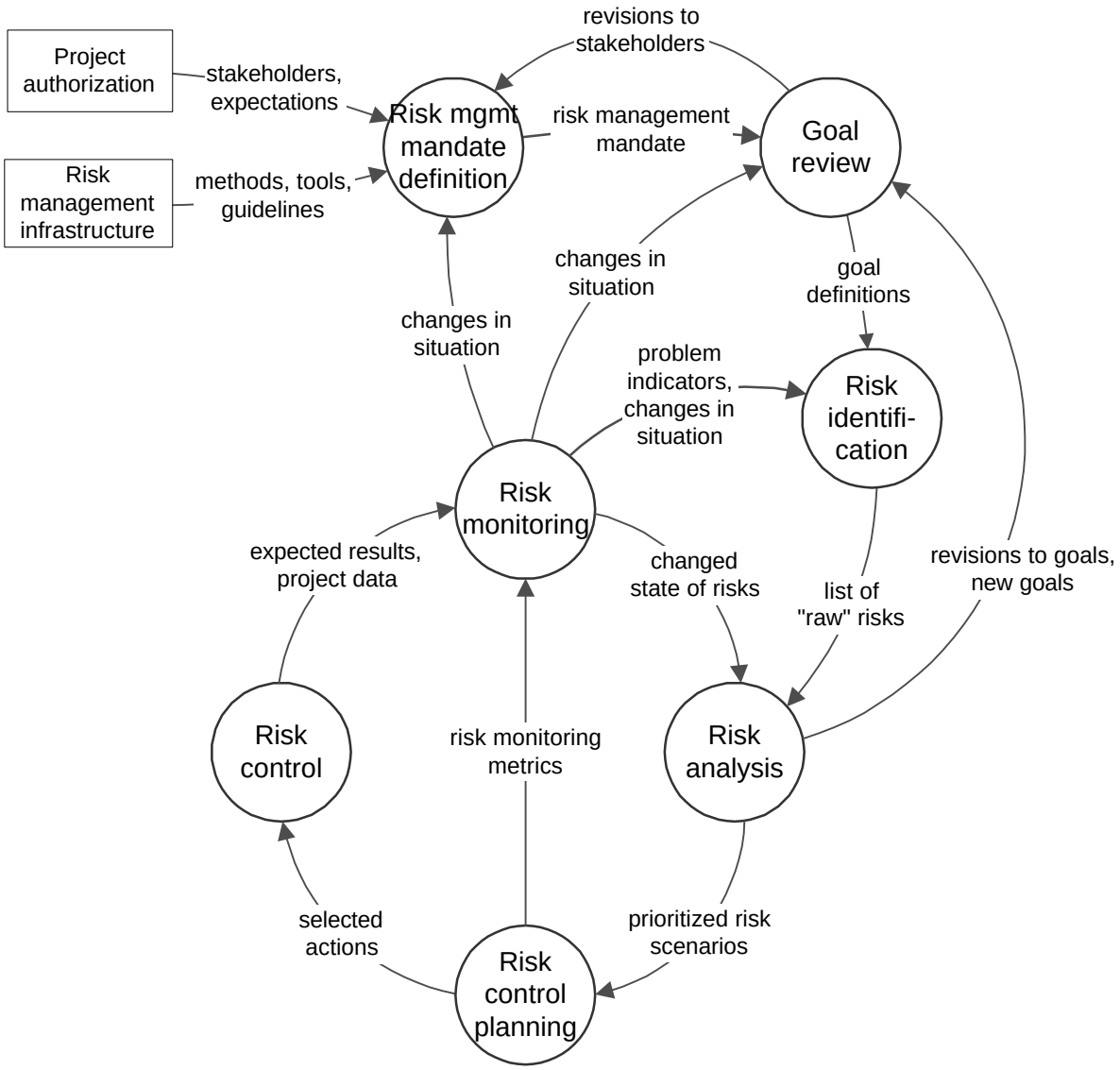


Figure 6: The Riskit risk management cycle

We have presented summary descriptions of the Riskit sub-processes in Table 5, which presents summaries of the activities in the Riskit process, as well as the main output of each activity. Each process will be defined in more detail in the following sections.

Riskit step	Description	Output
Risk management mandate definition	Define the scope and frequency of risk management. Recognize all relevant stakeholders	Risk management mandate: why, what, when, who, how, and for whom
Goal review	Review the stated goals for the project, refine them and define implicit goals and constraints explicitly. Analyze stakeholders' associations with the goals.	Explicit goal definitions
Risk identification	Identify potential threats to the project using multiple approaches.	A list of "raw" risks.
Risk analysis	Classify and consolidate risks. Complete risk scenarios for main risk events. Estimate risk effects for all risk scenarios Estimate probabilities and utility losses of risk scenarios.	Completed Riskit analysis graphs for all analyzed risks. Ranked risk scenarios.
Risk control planning	Select the most important risks for risk control planning. Propose risk controlling actions for most important risks. Select the risk controlling actions to be implemented.	Selected risk controlling actions.
Risk control	Implement the risk controlling actions.	Reduced risks.
Risk monitoring	Monitor the risk situation.	Risk status information.

Table 5: Overview of outputs and exit criteria of the Riskit process

The Riskit process presented in this section can also be seen from the perspective of artifacts it produces. This perspective is useful in determining how changes in one artifact or its component should be propagated to other components. Figure 7 presents this view of the artifact relationships.

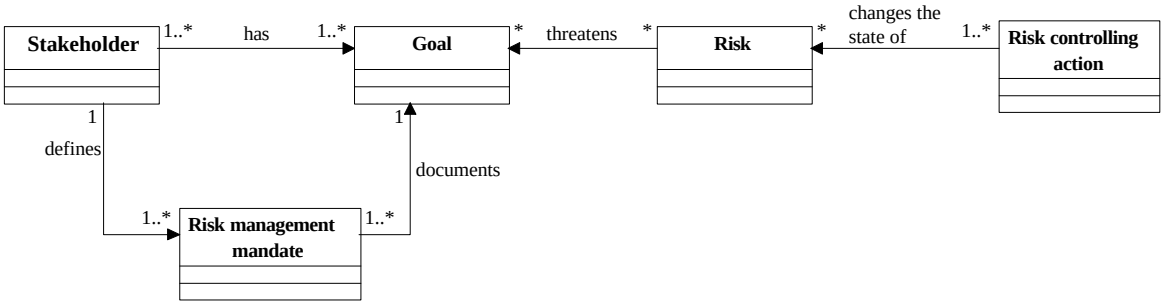


Figure 7: Riskit process artifact dependencies

The point of Figure 7 is that a change in one of the components should trigger re-evaluation of items that are dependent on the changing item. For instance, if a new stakeholder is recognized, goals, risks, and risk controlling actions should reviewed and analyzed. In practice this is done by reinitializing corresponding Riskit processes.

6.1 Risk Management Mandate Definition

The risk management mandate is a project specific statement on the scope of risk management in a project. The responsibility of defining the risk management mandate belongs to the owner of the project, i.e., the person or organizational unit that authorizes or funds the project or who will use or sell its results. Typically project owner is the person or group of people to

whom the project manager reports, e.g., a project steering group. The process definition information for this process has been presented in Table 6.

The risk management mandate definition process is initiated when any of the three entry conditions listed in Table 6 are met, i.e., when the project is initiated or when there has been a change in stakeholders or in the overall risk level of the project. Stakeholder changes may be identified in other parts of the process, especially in the goal review and definition process and in the risk identification and analysis processes. The acceptance of stakeholders into the risk management mandate needs to be controlled by project owner and therefore it must be handled by this process. Likewise, if there has been a significant change in the overall risk level in a project, or the risk analysis has revealed that initial assumptions about the risk levels are not valid, the risk management mandate may need to be revised. For instance, additional resources may need to be allocated or specific areas of risk may be given a higher priority or more frequent reporting cycles.

Purpose:	Define the scope and frequency of risk management.
Description:	Defines the responsibility, authority, scope and focus of risk management in a project.
Entry criteria	[project planning has been initiated] OR [stakeholders have changed] OR [project's overall risk level has changed] OR [stakeholder's risk tolerance has changed]
Input:	Project authorization information: goals, resources, schedule, budget. Organization's risk management policy and practice.
Output:	Risk management mandate.
Methods and tools:	NA
Responsibility:	Project owner or project manager.
Resources:	Project owner, project manager.
Exit criteria:	Risk management mandate documented and approved.

Table 6: The process definition information for the *risk management mandate definition* process

The risk management mandate defines which stakeholders are to be defended in risk management, stakeholders' priorities, which risks may be excluded from project management's risk management scope (e.g., organization management may be willing to take responsibility of some risks without burdening project management with any risk controlling responsibility), and how often and on what level detail should risks be managed. The risk management mandate may also define any other procedures that are not addressed by the existing risk management infrastructure, i.e., the current methods, processes and tools that have been defined for risk management. A template for defining the risk management mandate is presented in Table 7.

Risk mgmt mandate attribute	Description	Example
Objectives	Statement of main objectives for risk management.	*"The objective of risk management in this program is to prevent major risks from occurring, keep project owners informed of the risk situation in the program and, when feasible, estimate the size of risks in the program."*
Scope	Definition of scope for risk management: what areas of risk should be covered and what level of detail should be involved.	*"The program is responsible for managing all technical, personnel and project management related risks."*
Risk management authority	Definition of authority or budget available for risk management.	*"The program manager has been allocated 12 person months of developer time for implementing risk controlling actions. Additional risk controlling action expenditures have to be approved by the steering group."*
Accepted risks	Description of risks that the project owners have accepted and are thus excluded from project's normal risk management scope.	*"Management takes responsibility for risks that deal with competitive situation changes and possible corporate reorganization."*
Risk management procedures	Description of the risk management procedures, methods or techniques to be used.	*"The standard, corporate risk management procedures are followed in the program with following modifications:* • *A dedicated risk identification session is held every two months* • *Top 10 lists and corresponding risk controlling actions are included in monthly reports."*
Stakeholders	Identification of stakeholders and their priority.	*"The stakeholders covered in risk management, in order of their importance, are customer, division management, and sales division."*

Table 7: Risk management mandate definition template and example

The risk management mandate definition process is concluded when all items listed in Table 7 have been addressed and approved.

6.2 Goal review

Risks do not exist without a reference to goals, expectations or constraints that are associated with a project. If goals are not recognized, risks that may affect them may be ignored totally or, in the best case, they cannot be analyzed in any detail as the reference level is not defined. Some of a projects goals typically have been explicitly defined but many relevant aspects that influence management decisions may be implicit. Therefore, it is necessary to begin the risk management process by a careful review, definition and refinement of goals and expectations that are associated with a project. The definition of the goal review process is given in Table 8.

Purpose:	Define project's goals explicitly. Recognize all relevant stakeholders and their associations with the goals.
Description:	Existing goal definitions are reviewed and refined, if necessary, implicit goals are identified and defined. Different stakeholders are identified, their importance or priority defined, and their association and expectation levels with goals
Entry criteria	[project planning has been initiated] OR [new goals or stakeholders are identified] OR [a change in goals or stakeholders has been recognized]
Input:	Project authorization information: goals, resources, schedule, budget. Risk management mandate.
Output:	Goal definitions.
Methods and tools:	GQM [4,6]
Responsibility:	Project manager.
Resources:	Project owner, project stakeholders, project personnel.
Exit criteria:	Goals are explicitly documented and participants agree with their definition.

Table 8: The process definition information for the *goal review* process

In the Riskit method we identify three different types of goals. We use the term goal to refer to any of them, i.e., a goal is a general statement of purpose, direction or objective. When defined more accurately, we have found it useful to classify goals into three categories:

Objective: A goal that has an achievable, well-defined target level of achievement, e.g., "drive from A to B in one hour."

Driver: A goal that indicates a "direction" of intentions without clearly defined criteria for determining when the "goal" has been reached, e.g., "drive from A to B as

Constraint: A limitation or rule that must be respected, e.g., "while obeying all traffic

The review of projects' goals often leads to definition of some additional, previously implicit objectives, drivers and constraints. The purpose of this step is to produce formal definitions of these issues for the stakeholders that the project manager must satisfy. The goals are expressed using the template presented in Table 9.

Goal attribute	Description
Name	Name of the goal.
Type of goal	Objective / driver / constraint
Description	Description of the goal.
Stakeholder(s)	Names of the stakeholders for the goal that are interested in it.
Measurement unit	Measurement unit(s) used for the goal (e.g., $, date, or person-month).
Target value	Target value for the goal. Relevant for objectives and possibly for constraints.
Direction of increasing utility	Definition of whether an increase or decrease in goal value increases the utility. I.e., whether an increase in goal metric is good or bad. Stated as "growing" or "decreasing".
Required value range	Minimum or maximum value required for the goal, if applicable.

Table 9: Goal definition template

As Table 9 indicates, goals are linked to different stakeholders that are associated with a project. This information will later be used in risk analysis to compare and rank risks. If new stakeholders are identified, they are defined and documented as described in the risk management mandate definition process. From the perspective of our process definition, a change in stakeholders initiates a new instance of the risk management mandate definition process.

The relationships between goals and stakeholders can also be documented using a stakeholder-goal priority table presented in Table 10. Such a table allows approximate prioritization of goals for each stakeholder: each cell in Table 10 documents relative importance of goals for each stakeholder. It is important to point out that if such rankings are documented for stakeholders, each column should be read and interpreted independently. Priority values *between* stakeholders for a given goal cannot be derived from such information. In other words, goal priority rankings should be interpreted only within a single column, not across columns in Table 10.

As shown in Table 10, the relative priorities between stakeholders can also be documented in stakeholder column headings. This information is initially defined in the risk management mandate definition process.

Stakeholders: **Goals:**	Stakeholder A priority: 1	Stakeholder B priority: 1	...	Stakeholder X priority: 2
Goal 1	1	2	...	4
...	...	...	...	...
Goal n	NA	2	...	1

Table 10: An example of a stakeholder-goal priority table

The goal and stakeholder priority information is useful information for the risk analysis process as it allows more effective filtering and ranking of risks. Without such information project manager may be forced to make intuitive or undocumented judgment calls regarding which risks are selected for further analysis or how utility losses are prioritized. Note that it is

usually adequate to provide ordinal scale partial rankings of these items, either by using predefined categories (e.g., low, medium, high) or defining priorities for these items.

Most important goals are often defined in the project plan or the project contract. However, all of the goals may not be in these documents. For instance, efficient resource utilization may be an important consideration for a contractor but this typically is not considered a project goal. However, if these goals are real for some of the stakeholders in the project, they must be included in the risk management process. Goals can typically be found in the following areas:

- schedule;
- resources used, most often personnel time;
- cost of development;
- product requirements, which can include both functional and other quality characteristics;
- resource utilization; and
- technical constraints, such as hardware platforms, operating systems and use of particular software tools.

The goal review can be considered completed when project manager and stakeholders have reached an agreement on the goals and they are formally defined. However, the goal definition process may often need to be re-initiated as new goals are identified during the risk analysis process.

6.3 Risk Identification

The purpose of the risk identification process is to identify potential threats to the project and its stakeholders. Table 11 presents the process definition information for this process. As Figure 6 and Table 11 show, the risk identification process is initially carried out in the beginning of the project as its results are fed into the risk analysis process. The risk identification process is activated again when either of the two other conditions in the "entry criteria" row are met: if stakeholders or goals change or if the project situation changes.

The goal of the risk identification process is to produce a comprehensive list of all reasonable risks to the project. The mental mode of the identification process is to suggest many potential risks, not to analyze them. Analysis and filtering of risks produced will take place in the next step of the Riskit process. There are various techniques that can be used to facilitate effective risk element identification, such as brainstorming, checklists [11,13,25,32], critical path analysis, even simulation and benchmarking [11]. Based on our experiences, we recommend that informal techniques, such as brainstorming, are used in the beginning of risk analysis and more formal approaches are introduced gradually. This approach does not create initial bias in risk identification and it introduces formality as participants may start to lose their vigor in identification.

The risk list that is produced should be numbered or coded so that all risks can be traced throughout the risk management process.

Purpose:	Identify potential threats to the project.
Description:	Identify a large number of possible threats to the project using multiple approaches.
Entry criteria	[project planning has been initiated] OR [new goals or stakeholders are identified] OR [a change in goals or stakeholders has been recognized] OR [the time interval stated in risk management mandate has elapsed] OR [a significant change is project's situation has been recognized]
Input:	Project authorization information: goals, resources, schedule, budget. Risk management mandate. Risk checklists, general [13,32] or organization-specific [12]. Lessons learned reports from similar projects.
Output:	A "raw", numbered list of risks.
Methods and tools:	Brainstorming techniques. Goal and stakeholder driven identification approaches. Meeting aids. Interviews.
Responsibility:	Project manager.
Resources:	Project personnel. Risk management facilitator.
Exit criteria:	The marginal yield of risk identification approaches zero, even when identification techniques are changed, OR time or effort allocated for risk identification runs out.

Table 11: The process definition information for the *risk identification* process

There are two possible strategies for concluding risk identification process. The recommended approach is to conclude when no new reasonable risks are identified when alternative identification techniques are used. Such a situation would suggest that the identification process has exhausted all reasonable risks and further effort is no longer cost effective. However, this approach may be costly and subject to participant fatigue. An alternative approach is to set a predefined time limit, such as a single three-hour session, for risk identification. This approach can be justified by arguing that it is likely that most relevant risks are identified in the beginning and if adequate time is allotted, any remaining risks are not likely to be critical. Considering that risk identification is a critical activity and it is not particularly expensive, we recommend that a conservative approach is used in terminating the risk identification process, i.e., it is better to keep on identifying new risks a bit too long than to stop the process too early.

6.4 Risk Analysis

Risk analysis is a process where the "raw" risks from the risk identification process are grouped, filtered and prioritized. The goal of this activity is to provide detailed descriptions of projects' risks so that highest risk scenarios and appropriate risk controlling action can be planned and implemented in the next step of the Riskit cycle. Table 12 presents a summary of the risk analysis process.

Purpose:	Understand and prioritize risks.
Description:	Analyze risks and their components so that their probabilities and impacts can be assessed and most important risks recognized.
Entry criteria	Potential new risks are identified.
Input:	A list of risk items.
Output:	A prioritized list of risk scenarios.
Methods and tools:	Riskit analysis graph. Multiple criteria decision making tools. Riskit Pareto ranking technique.
Responsibility:	Project manager.
Resources:	Selected project personnel. Risk management facilitator.
Exit criteria:	Participants agree on the priority of the most important risks.

Table 12: The process definition information for the *risk analysis* process

Three main activities can be identified in the risk analysis process. First, raw risk items are clustered into sets, second, selected risks are documented as risk scenarios, and third, risk scenarios area ranked. Risk clustering and risk scenario development are iterative process that interact with each other: developing a risk scenario may prompt revisions in risk clusters and vice versa. These relationships between the processes are represented in Figure 8. These processes will be discussed in the following sections.

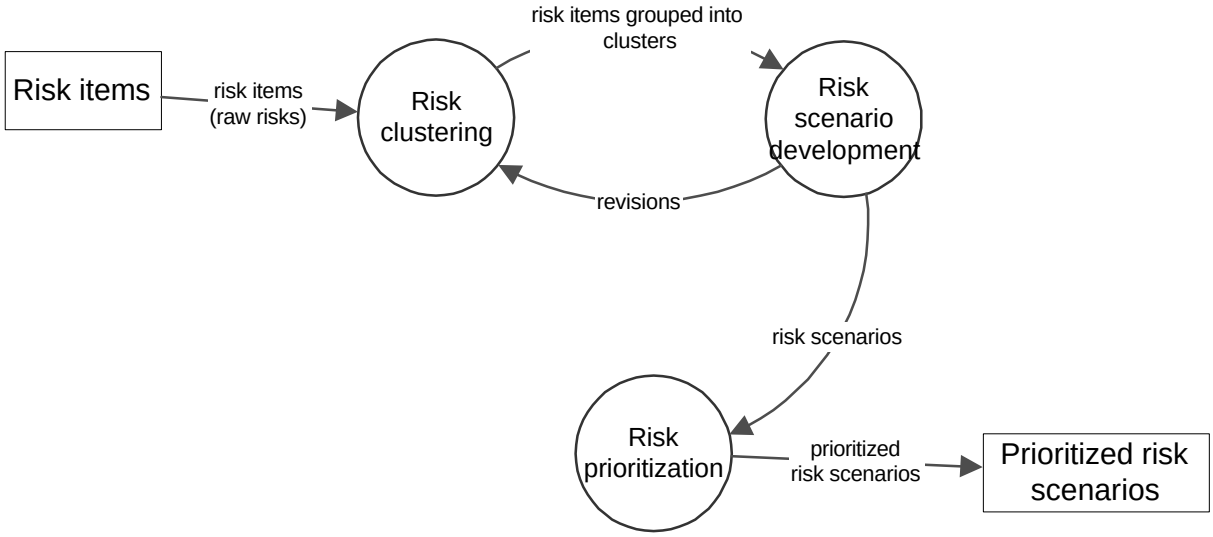


Figure 8: Sub-processes in risk analysis process

6.4.1 Risks Item Clustering

As the risk list produced by the risk identification process is an "un-analyzed" list of risks, it can contain redundant and overlapping items, as well as items on different levels of abstraction. If the risk identification process produced many such items, e.g., over 20, these risk items should be clustered into sets that contain similar risk items. This process is called risk item clustering and we have presented the process definition for it in Table 13.

Purpose:	Group “raw” risk items into clusters.
Description:	Group, decompose, merge or delete risk items into manageable clusters.
Entry criteria	Potential new risk items are identified.
Input:	A list of risk items.
Output:	Risk items grouped into clusters.
Methods and tools:	Word-processor, drawing tools.
Responsibility:	Project manager.
Resources:	Selected project personnel. Risk management facilitator.
Exit criteria:	All risks are included in the cluster set and number of clusters is manageable.

Table 13: The process definition information for the *risk item clustering* process

The purpose of risk item clustering is to provide a manageable intermediate step in risk management. The number of risk items produced in the risk identification process can be large and represent risks of different granularity. In many cases it is meaningful to cluster these items into sets that contain risks that relate to same area or are otherwise similar. Possible criteria for “similarity” include

- type of risk: technical, personnel, organizational, quality, schedule, functionality, product structure, etc. Some of these can be divided further.
- criticality: some risks may be considered obviously critical already at the risk clustering step
- stakeholders: risks may be grouped by stakeholders, i.e., risks affecting mainly a single stakeholder are grouped into one set.

The definition of “similar” is subjective judgment and not overly critical, as all risk clusters will be analyzed further and developed into specific risk scenarios in the next step. Risk clusters mainly provide a temporary structuring mechanism for the “raw” risk items produced in the risk identification process. More detailed analysis will be done in the scenario development process.

6.4.2 Risk Scenario Development

Risk scenario development provides the detailed documentation of risks that are selected for analysis. Risk scenarios are documented using the Riskit analysis graph (presented in section 5). One of the three different versions of the graph can be selected based on the level of granularity desired from the analysis, and the time available for the analysis. As a default, we recommend that the “normal” Riskit analysis graph is used (see Figure 3, page 13). We have presented a process definition for this sub-process in Table 14.

Purpose:	Develop risk scenarios for main risks.
Description:	Develop risk scenarios for main risks using the Riskit analysis graph.
Entry criteria	[risk clusters have become available] OR [new information becomes available and is not compatible with existing risk scenarios]
Input:	Risk items grouped into clusters.
Output:	Risk scenarios for most relevant risks.
Methods and tools:	Riskit analysis graph and drawing tool.
Responsibility:	Project manager.
Resources:	Selected project personnel. Risk management facilitator.
Exit criteria:	All selected scenarios are completed.

Table 14: The process definition information for the *risk scenario development* process

As there normally is limited time available for risk analysis, not all risk items from the risk identification process can be included in risk analysis. Therefore, selecting ("raw") risk items from risk clusters is an initial risk prioritization choice, yet this choice is made when the risks are not yet analyzed. To counter the possible bias caused by such an early selection, an adequate number of risk scenarios should be developed. Also, all risk items should be explicitly decided upon, they should not be left out of the analysis only because they got lost among other risk items. Our rule of thumb is to select most important scenarios from remaining risk clusters and keep on developing scenarios them until several most recent scenarios have not resulted in risk controlling actions that will be implemented. The rationale of this strategy is that if, after careful analysis, additional risk scenarios do not result in cost effective risk controlling action, they are not considered big enough risks by decision makers.

When risk scenarios are developed, the items in relevant risk clusters can be reviewed as candidates for risk elements. As defined in section 5, risk elements are defined column by column, as shown by an example in Figure 9. The example in Figure 9 represents two scenarios as the event "unrealistic effort estimation" has two potential reactions, "accept delay and added cost" and "allocate more resources," both with different effect sets.

The first step in risk analysis, classifying risks into risk factors and risk events, is based on the risk list produced during the identification process. The categorization is based on the definitions given in section 5 and results are documented in the Riskit analysis graph (Table 2). An example of a Riskit analysis graph is given in Figure 9.

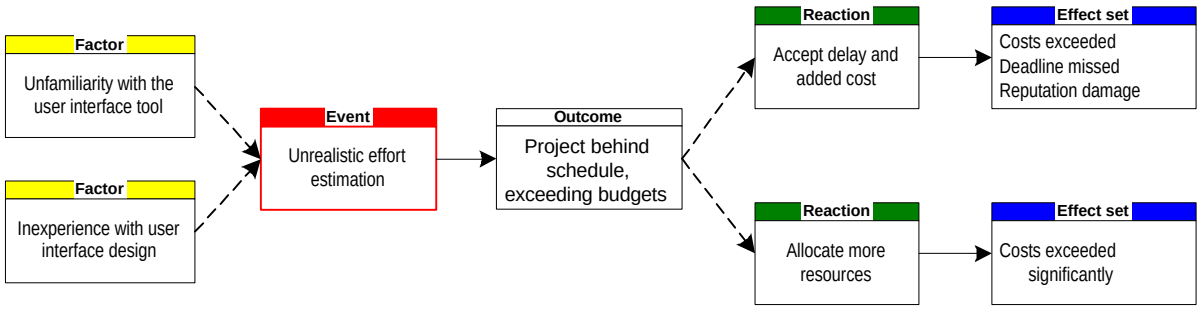


Figure 9: Example of the Riskit analysis graph

The Riskit analysis graphs can also be expressed in textual form using indentation, as is shown in Figure 10, using the same example as in Figure 9. However, the main disadvantage of this textual representation is that it is difficult –and sometimes impossible –to represent complex relationships between risk elements without duplicating them. For instance, when a risk factor influences several risk events, the textual form may become impractical. In such situations, one solution is to duplicate the risk factor items at each risk scenario. This reduces the visual power of representation and may create consistency problems when graphs are revised. Although we have developed tabular alternatives that avoid the redundancy problem, they seem to increase the complexity of the representation unnecessarily and as of now we are not recommending their use.

Factors:
- Unfamiliarity with the user interface tool
- Inexperience with user interface design

Event: Unrealistic Effort estimation
Outcome: Project behind schedule, exceeding budgets
Reaction: Accept delay and added cost
Effect set:
Costs exceeded
Deadline missed
Reputation damage
Reaction: Allocate more resources
Effect set:
Costs exceeded significantly

Figure 10: Textual version of the Riskit analysis graph

The main task of scenario development is not to map each risk item produced in the risk identification process into a Riskit analysis graph. Instead, judgment must be used to select scenarios that capture essential and representative future risk scenarios. The following criteria can be used when determining whether a scenario represents an appropriate set of future events:

- The risk event in the scenario represents event instances that are similar in nature and their probability can be estimated.
- The range of potential effects in the scenario is not extreme.
- Potential risk controlling actions are same or similar for all scenario instances.

If there is fuzziness or wide range of possibilities with either of the above criteria, the scenario should be potentially decomposed into two or more scenarios.

Each risk scenario is documented in the Riskit analysis graph and, depending on the available time and resources, each risk element is defined using the risk element definition templates presented in Table 15, Table 16, Table 17, and Table 18.

Risk factor attributes	Description
Name	Name of the risk factor to be used as an identifier.
Description	Description of the risk factor.
Normal/assumed level	Description of the “normal” level for the risk factor.
Project’s risk factor state	Description of the risk factors value for the project

Table 15: Risk factor definition template

Risk event attributes	Description
Name	Name of the risk event to be used as an identifier.
Description	Description of the risk event.
Probability of occurrence	Assessment of the probability of the event occurring.
Uncertainty of the estimate	Assessment of the uncertainty in the probability assessment.
Information source	Description of sources of information about the risk event for monitoring the changes in the probability or event occurrence.
Timeframe	Estimate of when the occurrence of risk will take place.

Table 16: Risk event definition template

Risk outcome attributes	Description
Name	Name of the risk outcome to be used as an identifier.
Description	Description of the outcome. A description of the project state after the event but before any other action is taken.
Certainty of the outcome	Assessment of the probability of the outcome if the risk event occurs (when not deterministic).

Table 17: Risk outcome definition template

Risk Reaction attributes	Description
Name	Name of the risk reaction to be used as an identifier.
Description	Description of the reaction. A description of the line of action or procedures that may be carried out if an event occurs.
Rationale	Description of the rationale for taking the action.

Table 18: Risk reaction definition template

The final step in risk scenario development is to estimate effects of scenarios. Effects are collected into sets and associated with each scenario. Effects are described through goals: each goal that is affected by a scenario is included in the effect set description and the effect is stated as a deviation from the goal or, in the cases of a driver, deviation from is expected. Depending on the estimation methods and tools available, the effects can be stated qualitatively (e.g., as textual descriptions or classifications high/medium/low) or quantitatively. Ranges can be expressed as well, if participants consider this necessary. Table 19 presents a template for describing scenario effects.

Note that effects should describe the net effect of the scenario after the event has occurred and reaction has taken place. It is often the case that not all goals are affected by a risk scenario, and sometimes the effects may be positive for some goals (e.g., loss of personnel may reduce costs while delaying schedule and limiting functionality).

Risk Effect set attributes	Description
Name	Name of the risk effect set to be used as an identifier.
Description	Itemized description of the effects. The effect description can be qualitative, i.e., a written characterization of the effect, or a quantitative estimate of the effect. Effects can also be described as ranges. All effects are defined in terms of the goals they affect. If an effect that is not previously documented as a goal is recognized, corresponding goal definition must be made.

Table 19: Risk Effect set definition template

6.4.3 Risk Prioritization

As resources for risk management are limited, it may not be feasible to mitigate or analyze all risk scenarios. Instead, one should focus on most important risks and spend relatively more time and resources on their management. In order to do this, it is necessary to rank the risk scenarios. Thus, the final step in risk analysis is to prioritize risk scenarios. The process definition for the risk prioritization process is given in Table 20

Purpose:	Prioritize risk scenarios.
Description:	Based on the estimates for probability and utility loss for each scenario, prioritize scenarios with respect to their seriousness.
Entry criteria	[Risk scenarios have been completed] OR [new risk scenarios have been defined] OR [new information becomes available and is not compatible with existing prioritization]
Input:	Risk scenarios.
Output:	Partially prioritized risk scenarios.
Methods and tools:	Riskit Pareto ranking technique.
Responsibility:	Project manager.
Resources:	Selected project personnel. Risk management facilitator.
Exit criteria:	Selected scenarios have been ranked as well as available data allows.

Table 20: The process definition information for the *risk prioritization* process

In order to prioritize risk scenarios it is necessary to estimate the probability and utility loss associated with each scenario. These two estimation problems have different kinds of inherent difficulties. Probability estimation is difficult because little historical data may be available and event probabilities, in principle, are unknowable in a changing environment [23,30]. Utility loss estimation is difficult because there are multiple factors to be considered and the exact shapes and forms of stakeholders' utility functions are not known. We will discuss the estimation problems for each aspect of risk separately in the following.

If historical data about risks is available and if it can be safely assumed that the risk situation has not changed from the projects where the historical data was collected from, a frequency based interpretation of probability [22] can be used and past risk occurrences can be used as an estimate of the probability. However, in software engineering context such data hardly ever exists in adequate volume in order to be statistically reliable and the assumption about status quo is rarely realistic. Therefore, while historical data can be used as input to the estimation process, subjective probabilities, i.e., degrees of belief [22], are often the only

source for probability estimates. At the same time, it has been shown that direct query of numerical or verbal ratings of probabilities are not reliable [43] and more systematic approaches are relatively costly [34] for most software projects. Unless adequate time can be spent in probability estimate elicitation to control biases [43], we recommend that scenario probabilities are ranked subjectively, resulting in a ordinal scale rankings between scenarios. The use of ordinal scale rankings makes it clear that rankings are based on incomplete information and the impact of possible estimation errors or biases is reduced. If rankings are inconclusive between some scenarios, they can be evaluated further.

Risk scenario probabilities are estimated by ranking them based on their subjective probability of occurrence. We recommend that a pair-wise ranking approach [41] is used instead of using predefined ordinal scale values, due to potential problems with their interpretation [34,43]. Using this approach the risk scenario ranking is done as follows:

1. Participants are asked to individually rank scenarios in decreasing order of subjective probability. To ease this process and to increase the accuracy of rankings, a pair-wise comparison approach can be used, such the AHP method [41].
2. Resulting rankings are compared and discrepancies highlighted.
3. Discrepancies are discussed and resolved by consensus.

If consensus cannot be reached in a discussion, two strategies can be used to resolve the issue. First, the ranking of the debatable items can be increased so that a conservative interpretation is used: it is better to err on the side of caution than to assign too low a ranking. Second alternative is to group debatable items into same ranking category, i.e., collapsing rank categories into one category.

When a scenario contains only one probabilistic element, i.e., a single risk event followed by deterministic outcome, reaction and effect set, the probability of the risk event and the risk scenario are the same. Probability estimation becomes more difficult when a scenario includes probabilistic elements, such as alternative outcomes or reactions. If reliable numerical (ratio scale) estimates for probabilities can be elicited and the probabilistic elements in the scenario are disjoint, the scenario probabilities can be calculated using straight-forward conditional probability calculations. However, if such estimates are not available –which we believe is often the case –scenario probabilities must be estimated separately for each scenario. Given the increased complexity of such a situation, the estimation process should be carefully conducted so that complexity does not reduce estimation reliability unnecessarily.

The resulting list of scenario probabilities will be a partially ordered set, where some scenarios may be assigned into a same probability rank.

Estimation of the utility loss for each scenario is also constrained by the time availability for the analysis. In principle, utility losses between scenarios could be derived using various multiple criteria decision making tools [22,23,40]. However, given the possible fuzziness involved in the effect sets and cost of applying such methods we recommend that similar ranking approach is used to rank utility losses between scenarios.

Utility losses of scenarios are ranked separately for each stakeholder. However, if stakeholder goal priorities are identical or very similar, such stakeholders can be ranked together. Such a joint ranking should be done cautiously because even when the goal priorities are similar, the underlying utility functions may be quite different. Merging stakeholder views, therefore, is a compromise that may sacrifice accuracy of stakeholder rankings.

Once the rankings for probabilities and utility losses have been obtained for all scenarios, they can be ranked. The concept of expected utility loss can be used to prioritize scenarios if both probability estimates and utility loss estimates have been estimated using distance or ratio scale metrics [21]. In such a case the *expected utility loss* of a risk scenario can be calculated by the following formula:

expected utility loss(RS) = probability(RS) * utility loss(RS)

where 'RS' indicates a given risk scenario.

However, this formula can rarely be used due to difficulties and costs involved in obtaining the distance or ratio scale metrics for the factors in the formula. Therefore, we have developed an alternative scenario ranking technique that can deal with ordinal scale estimates for probability and utility loss, yet provide reliable rankings of scenario risks. We call the ranking technique *Riskit Pareto ranking technique*. The Riskit Pareto ranking technique uses the probability and utility loss rankings of scenarios and searches for scenarios that are Pareto efficient over other scenarios, i.e., scenarios that are on the Pareto-efficient frontier[7] w.r.t. utility loss and probability ranks that have been used. Risk scenarios that are on the Pareto efficient frontier are not worse on either probability or utility loss estimate than any other risk scenario. This approach can be visualized with a simple table, as shown in Table 21: scenarios are positioned on the Riskit Pareto ranking table according to their rankings w.r.t. probability and utility loss. A scenario's Pareto efficiency over other scenarios can be easily assessed in the table: it is Pareto efficient if no other scenarios are in cell above it or left of it.

Using the Riskit Pareto ranking technique results in a partial ranking of risk scenarios, i.e., priorities for some scenarios can be defined but some scenarios' relative priority remains unknown. While the complete prioritization of scenarios would be desirable, the input data leading to the prioritization does not normally allow it.

In Table 21 scenario 1 is Pareto efficient over all other scenarios. The remaining scenarios can be only partially ranked based on the available information. The priority between scenarios 2 and 4 cannot be established but one can say that Scenarios 2 has higher priority than scenarios 3, 5, 6, and 7; and that scenario 4 has higher priority than scenarios 5, 6, and 7. The significance of these partial rankings is that they guide the focus of risk management to scenarios that have been reliably prioritized over other scenarios, given the information available. The risks should be considered for risk controlling action planning in their order of priority.

[7] Pareto-efficient frontier consists of alternatives that are Pareto optimal over other points in a set. An alternative *a* is considered Pareto optimal over *b* when $\forall$ *i* so that $a_i >= b_i$ and $\exists$ *i* so that $a_i > b_i$ for all i = 1, 2, 3, ..n, where n is the number of criteria involved [22,26].

Risk scenario Utility loss	Risk scenario probability				
	rank 1	*rank 2*	*rank 3*	…	*rank n*
rank 1	scenario 1	scenario 2		…	
rank 2			scenario 3	…	
rank 3	scenario 4	scenario 5	scenario 6	…	
…	…	…	…	…	…
rank m		scenario 7		…	

Table 21: Risk scenario ranking table using Pareto-efficient sets

Note that Table 21 may tempt some users to rank all risk scenarios on the same diagonal as "equal" or "indifferent" and use this information to derive further rankings on the scenarios. According to this view, using the Table 21 as an example, one would assume that since scenarios 3 and 5 are "indifferent" and scenario 5 is higher risk than scenario 7, scenario 3 is higher risk than scenario 7. Such an interpretation would also seem intuitively correct, as people easily associate equal distance between the rank categories in the Riskit Pareto ranking table. However, we would caution against such an interpretation because ordinal scale metrics cannot convey enough information to assume transitivity of the "indifferent" relationship between scenarios. Since transitivity cannot be assumed, such logical conclusions are not justifiable[8].

The risk scenario rankings that are produced are stakeholder dependent. If more than one stakeholder is supported in the analysis, a corresponding number of utility loss rankings should be performed. However, if stakeholders have identical or similar goal priorities (see Table 10), their utility loss rankings can be done can be merged to save time and reduce complexity of results[9]. This stakeholder view can be used in the risk control planning process to decide whether controlling actions for a risk scenario should be taken, what controlling actions should be taken and who should be covering the costs for them.

Once risk scenarios have been prioritized, even though partially so, the partially prioritized list of scenarios can be given as input to the next process in the Riskit cycle –risk control planing –and the risk analysis process can be terminated.

6.5 Risk Control Planning

The goal of risk control planning activity is to determine which risk control activities are necessary to take. The main issues in are the identification of which risks pose greatest threats and the selection of appropriate risk controlling actions to mitigate them.

[8] It is not safe to assume that relationships between scenarios 3 and 5 is that of "equivalent" nor that the relationship would be transitive. The priority of scenarios 3 and 5 is unknown and thus it cannot be used to draw conclusions on other priorities. For example, it would be wrong to conclude that because scenario 2 has higher risk than scenario 3 and because scenario 2 "is kind of same as" scenario 4, therefore scenario 4 has higher risk than scenario 3.

[9] It should be noted that this may cause error in rankings: although goal rankings may be similar, stakehoders' utility functions may be different and result in different utility rankings.

Purpose:	Propose and select cost effective risk controlling actions.
Description:	Define, prioritize and select risk controlling actions for the risk scenarios that have been considered most important.
Entry criteria	Important risk scenarios have been identified.
Input:	Partially prioritized risk scenarios.
Output:	Selected risk controlling actions. Risk monitoring metrics.
Methods and tools:	Riskit element review. Riskit controlling action taxonomy.
Responsibility:	Project manager.
Resources:	Selected project personnel. Risk management facilitator.
Exit criteria:	All selected risk scenarios have been addressed.

Table 22: The process definition information for the *risk control planning* process

Accomplishing these goals requires that both risk scenarios and risk controlling actions can be ranked or quantified. In most cases neither task is trivial and we recommend the use of systematic approaches for ranking risks and risk controlling actions. Thus, risk control planning involves two main activities: defining possible risk controlling actions and selecting cost-effective risk controlling actions to be implemented. While these two activities are discussed sequentially in the following sections, they are very much linked to each other. In fact, they should be seen as concurrent activities with continuous information exchange and incremental refinement.

6.5.1 Defining Risk Controlling Action

Once the high-risk scenarios have been selected, possible controlling actions are proposed for each of them. Identifying possible controlling actions is a creative process and can be carried out in a free format manner. However, in order to ensure consistency and adequate consideration for all possible options we have developed two complementing techniques that can be used to support the identification of potential risk controlling actions. These two techniques are called the *Riskit element review* and the *Riskit controlling action taxonomy*. We will introduce both approaches in the following.

The Riskit element review is based on the risk elements presented in the Riskit analysis graph. This technique simply calls for a focused review of all risk elements in a scenario and prompts participants to consider ways to influence the elements either by controlling them, finding alternatives or preventing them. This review can be supported by questions presented in Table 23.

Riskit element	Possible focusing review questions
Risk factor	• Can some risk factors be eliminated? • Can the situation described by some risk factors be improved or corrected? • Could the influence of current risk factors be reduced? • What other factors might compensate for influence of current risk factors?
Risk event	• What could be done to reduce the probability of risk event occurring? • Can there be a trial run? • Is training required? • Should the technology be evaluated, a prototype developed? • Can we learn from other people of projects?
Risk outcome	• Can alternative outcomes be created, e.g., more people assigned or trained?
Risk reaction	• What other reactions might be possible, can we do now to make them available? • Are more effective reactions possible? • Should we do more than just contingency plans?
Risk effect	• Can we compensate effects by some other means? • Can we protect some goals by some specific actions? • Are all goals equally critical?
Utility loss	• Are all expectations realistic? • What effects are not critical for utility loss? • Are there ways to reduce long term utility loss?

Table 23: Supporting focus questions for Riskit element review

We have synthesized and detailed a high level taxonomy of risk controlling options from contributions by Boehm and Charette [11,12,14-16]. This taxonomy is presented in Figure 11 and discussed in the following.

The first set of options in Figure 11, *no risk reducing action* means that an organization does not take any immediate action to prepare for risk or to reduce risk. This option does not reduce the risk itself but may provide more information as time goes on. This option is recommended when there is not enough information to make a decision or if risks are too small to justify any other risk controlling action. Further action can be taken if new information motivates it. This option can be broken further into three options.

The *wait and see* option can be used in two situations. First, it is a good option for all risks that are considered to be small enough not to require any other action. Second, it can also be considered when there are no inexpensive ways of obtaining additional information and a major part of the risk is in the uncertainty of the of risk size of risk. In other words, the ranges of estimates of risk are wide and management has no special reason to believe that higher risk estimates are probable. This option, in fact, would be the same as the reactive strategy we discussed earlier. Clearly, using this option to cover high uncertainty risks is, to say it simply, risky. A conservative approach would be to use some of the other options for high uncertainty risks.

Buying information is an option that is used when the management does not have enough information to decide what to do about a risk and there is a possibility to obtain more information. In principle, it is only a temporary option that results in a new decision as the information becomes available. After additional information becomes available, some of the other options are selected. Buying information can take many forms. Sometimes information can be literally bought from outside sources, such as market research organizations or by hiring a consultant that knows about the area that risk is relevant to. However, more typical

way of buying information is to develop prototypes, run simulations, initiate feasibility studies or conduct performance tests.

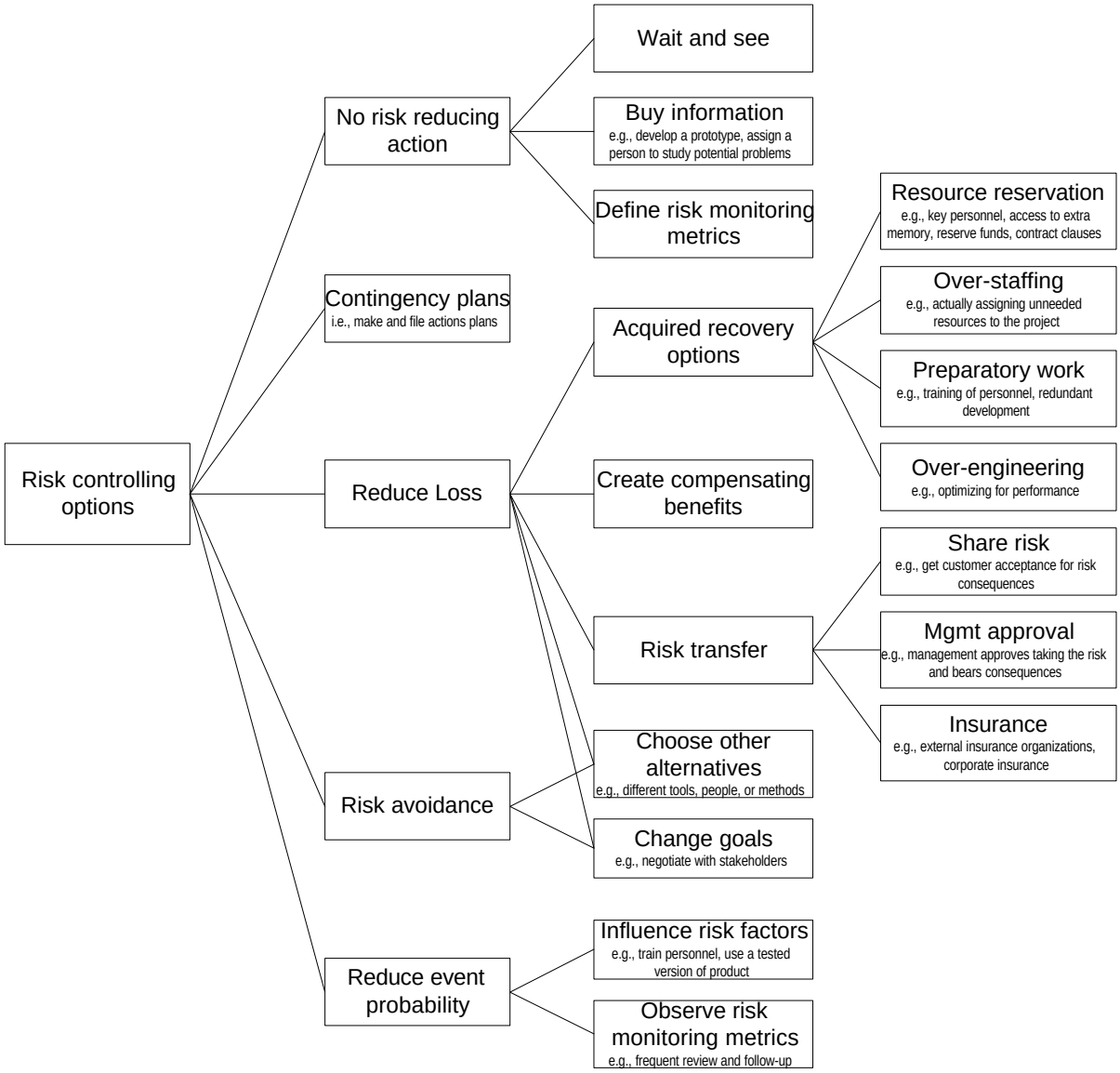


Figure 11: Options for risk management decision making

Defining risk monitoring metrics is an option that should be selected for all or most risk scenarios, regardless of the other risk controlling actions produced. Risk monitoring metrics may include existing process or product measures but they can also include new metrics, or even informal information items, such as "observing personnel morale" or "monitoring database technology developments." We recommend the use of GQM as a systematic method for defining such metrics, with modifications to include any information items as "leaves" in GQM trees, not just traditional metrics [4,6].

The second main option in Figure 11 is *contingency planning*. It means that recovery plans are made for a risk scenarios but no further action is taken. Strictly speaking, contingency plans have rather marginal effect on risk reduction as they mainly buy time and marginal effort in advance. However, since they change the mode of risk control towards

prevention this option has been listed separately from the previous option group. Contingency plans describe the actions that will be taken if the risk occurs. Plans are made and approved and they are put on hold to be used if risks occur. Contingency plans help organization make sure that there is a way to recover from the risk. Contingency plans can also be looked from another angle, they are, in effect, a way to detail the reactions and effects in risk scenarios.

The options under the term *Reduce loss* in Figure 11 refer to risk controlling actions that are aimed at mitigating the damage, i.e., effects or utility loss, caused by a risk. This option group has been divided further into five main groups, the two last ones are common to risk avoidance option group as well. The *Acquired recovery options* refers to a set of actions that buy options that can be used to limit the loss. They typically have a cost associated with them. The *Resource reservation* option refers to a situation where some resources are reserved for limiting the impact of risk if the risk occurs. Resources can be human, computer or financial. Resources are not used before the risk occurs but they are reserved so that they can be "called to rescue" when necessary. The second sub-option, *over-staffing*, may be introduced to make sure that more than one person knows enough about each area in the project. Whereas resource reservation does not necessarily affect the project budget, over-staffing is likely to do so. The third sub-option in this group, *preparatory work*, refers to some action that is done in preparation of risks. It is akin to contingency plans but the main difference is that some work is done just in case: if the risk does not occur this preparatory work will have been wasted. Note that preparatory work itself normally does not reduce the probability of risk event occurring, it just mitigates the effects. Finally, *over-engineering* means implementing some features in the product or design so that there will be alternative ways of action if the risk occurs. For instance, over-engineering could mean that extra effort is spent during design or coding to make sure that alternative system architecture or compilers can be used.

The second option under reduce loss category is called *create compensating benefits*. This means actions that reduce the utility loss that the effect set of a scenario would otherwise cause. For instance, if a risk scenario would result in two-month schedule delay, the utility loss could be reduced by monetary compensation, free training, or having technical personnel at a customer site to resolve problems locally during the delay period.

The third option under reduce loss category is called *Risk transfer* and it includes three different options. *Sharing risks* means obtaining conditional approval for risks from stakeholders or project owners. Sharing can happen, e.g., with customers or subcontractors of the project. Again, a critical issue is to analyze the risks well and communicate their significance to all stakeholders. *Management approval* is similar to sharing of risk but instead of negotiating with stakeholders, organization management takes the responsibility of risk. Using this option normally means that the existence of risk is acknowledged and but there are no feasible ways to reduce risk to an acceptable level from the project perspective. An example of such a risk might be a development of a Windows 95 compatible software version to be able enter the market when Windows 95 was released: at early stages of development there may not have been enough technical and schedule information about Windows 95 to justify development, yet efficient enough risk controlling action might have meant missing the window of opportunity. In such cases management can authorize the project to proceed in a line of action without spending time on controlling some "management approved" risks. Finally, the third option in this category is *insurance*, i.e., using external or corporate resources to insure for some risks. As real insurance options are rare in software development and as corporate, internal insurance schemes are, in effect, a variant of management approval, this option is rarely a realistic option.

Risk transfer should be used cautiously and limited to specific, clearly defined conditions or situations. Otherwise it can become a "free ticket" for project management not to worry about risks. This may require contractual negotiations or explicit agreement what risks are transferred and what are not. Even if risk transfer option is used, other risk controlling options are often applied.

The two options under *risk avoidance*[10] are also shared by reduce loss option. It contains two sub-options. *Choose other alternatives* refers to a actions where alternative approaches, methods, tools, resources or technologies are used. Each such alternative contains some characteristics that may contribute to some risks in a project, changing them may thus change the risk portfolio in a project. If decision about such alternatives are not yet made, the risk management process can easily contribute to the decision making process. If such decisions have already been made, it may be possible to consider revising such decisions, if that would prove to be a the cost effective risk controlling action.

Changing of goals is a potential and often effective risk controlling action. As we have pointed earlier, the definition of loss, and therefore risk as well, depends on the goals defined for the project. If these goals have been initially unrealistic, the correct and cost effective risk controlling action may be to change these goals. This requires negotiation with stakeholders and project owners and such negotiations should be supported by the results of the risk management process. While changing of goals may be a tempting, easy way out of a risky situation, it is clear that management and stakeholders do not want to see it applied too often.

Finally, the last option category in our taxonomy is *reducing event probability*. We have divided it into two options: *influence risk factors* and *observe risk monitoring metrics*. Influencing risk factors can address any risk factor included in a risk scenario and can propose improvements in risk factors that reduce event probabilities. For instance, if "inexperience in user interface design" is a factor for an event "user interface not accepted by users," the action to improve inexperience in user interface design might be to provide training for personnel, and the use of a user interface design tool might be a factor that compensates for the inexperience.

It is important to point out that both of the techniques presented here, the Riskit element review (Table 24) and the Riskit controlling action taxonomy (Figure 11) are not meant to be comprehensive or normative guides to arrive at an optimal list of risk controlling actions. Instead, they are meant to act as supporting tools that augment the risk controlling action planning and extend the search space for controlling actions. The most critical aspect of risk controlling action planning is the involvement of project personnel and their ability to innovate effective actions.

6.5.2 Selecting Risk Controlling Action

Once the potential risk controlling actions have been identified, the next task is to select most effective ones to be implemented. It is recommended that more risk controlling actions are produced than can be effectively implemented. This serves to confirm that the coverage of risk analysis and risk control planning has been adequate. If all proposed risk scenarios are selected to be targeted for risk controlling actions, it may indicate that risk scenarios not included in the risk control planning may need to be reconsidered. If all proposed risk controlling actions are

[10] Although risk avoidance could be considered a special, extreme case of either reduce loss or reduce event probability, it has been given its own category for two reasons: it is frequently mentioned by other sources [11], and it does represent a slight paradigm shift in thinking about risk controlling actions. Therefore, it is justifiable to separate it.

implemented, this signals that not enough risk controlling actions were proposed and some beneficial actions may have been missed.

In the Riskit method we use five criteria for selecting the risk controlling actions:

- Ranking of risk scenarios.
- Risk controlling action effectiveness.
- Resource availability.
- Stakeholder importance.
- Urgency of implementing the risk controlling action.

We will discuss these each in the following.

The first criterion, *focusing on highest risk scenarios*, is an obvious one, i.e., mitigate the highest risk scenarios. The highest risk scenarios are recognized by the risk scenario ranking done previously. The number of risks to be mitigated can be determined subjectively, be based on a predetermined threshold or criteria, or be based on a Pareto diagram and on the point of diminishing returns [35]. The most effective risk controlling action for each scenario is determined by estimating how much alternative actions reduce the expected utility loss. Given that expected utility loss is usually expressed as an ordinal scale rank between risk scenarios, the reduction of expected utility loss often remains a subjective judgment.

The focus on high-risk scenarios, however, is a slightly simplistic selection criterion. It does not account for the relative *efficiency of risk controlling actions* nor acknowledge possible resource constraints for implementing the actions. In principle, the risk reduction leverage proposed by Boehm [11] takes the effectiveness of proposed risk controlling actions into account. Within the context of the Riskit method, the risk reduction leverage should be applied to the utility loss of risk scenarios:

$$\text{risk reduction leverage} = \frac{\text{Expected utility loss}_{before} - \text{Expected utility loss}_{after}}{\text{Cost of risk controlling action}}$$

In other words, the reduction in expected utility is divided by the cost of the action that caused the reduction. However, the problem with this formula is that ordinal scale rankings of utility losses do not allow such a formula to be used. Even when distance or ratio scale estimates for utility loss were available, the accuracy of these estimates and those of cost estimations for controlling actions may make the formula impractical to use. In practice we recommend that the search for optimal risk is not even attempted, instead, relying on the principles of bounded rationality proposed by Herbert Simon [42], subjective judgment is used to select risk controlling actions that are considered effective enough in the light of available information.

The third selection criteria are *resource constraints*. This can refer to the risk management budget if it has been defined or to the amount of available resources and skills. These constraints may rule out some otherwise effective risk controlling actions. For instance, training all personnel fully on a new method might have a very high risk reduction leverage and reduce some key risks significantly but it may be unfeasible due to the cost and time delay involved.

Stakeholder importance and perspectives may also influence the selection of appropriate risk controlling actions. If stakeholders' risk scenario rankings differ, they may also have different preferences for implementing risk controlling actions. The process described here enables stakeholders to identify where their interests differ and where they are similar. For risk

controlling actions that compete for limited resources, stakeholders should negotiate and, if possible, consider taking responsibility or covering the cost of some risk controlling actions that primarily control risks that are most relevant to them.

Finally, the *urgency of implementing the risk controlling action* may strongly influence on what risks to mitigate and how. The risk controlling action urgency depends both on the time of the risk event occurrence and the time delay in implementing the risk controlling action, as Figure 12 shows. The time of risk event occurrence, naturally, influences the urgency. However, the risk controlling action impact delay is often omitted from risk timeframe analysis, although it can have a big impact on a situation as some risk controlling actions have long implementation delays. As time goes by, some risk controlling actions become infeasible if they are not considered early enough.

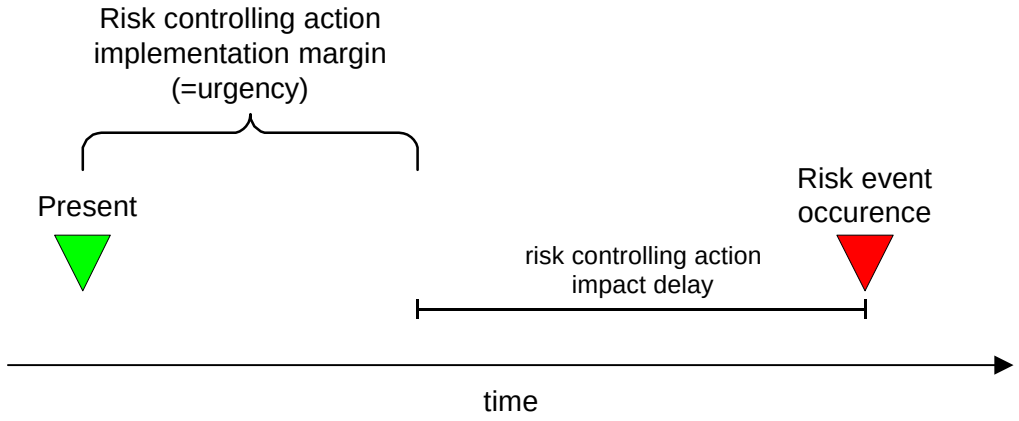


Figure 12: Risk controlling action urgency

We will use an example to illustrate the situation. Let us consider a risk event of "system architecture not defined by milestone 3." Whether this risk occurs or not will become clear at or near the milestone 3 which, in this example, is six months away and therefore not urgent. However, the two candidate risk controlling actions are "reuse the simpler architecture from previous system" and "recruiting of an experienced system architect." While the previous system's architecture can be reused with a short notice (perhaps within weeks), the recruiting and induction of new architecture expert could take several months. Therefore, the recruiting action has a higher urgency than reuse of old architecture.

The five criteria presented here for selecting risk controlling actions should be considered when deciding what action to take. While the importance of these criteria may vary between situations, based on our experience the risk ranking and risk controlling action urgency are often the most important criteria. In any case, professional judgment must be used to conclude what actions to take, as the criteria themselves does not necessarily provide unambiguous conclusions.

The risk control planning process can be concluded when all selected risk scenarios have been addressed by the process and a decision has been made whether to implement controlling actions for them or not.

6.6 Risk Control

Once the risk controlling actions have been defined and selected, they become a part of project management. Their actual implementation is a project and organization specific management

issue and the Riskit method itself does not provide detailed support on how this is done. However, the main requirements from this process are described in Table 24.

Purpose:	Implement risk controlling actions.
Description:	Implement the risk controlling actions defined by the risk control planning process.
Entry criteria	A risk controlling action has been selected for implementation.
Input:	Selected risk controlling actions.
Output:	Implemented risk controlling actions. Problems reports if problems arose in implementation.
Methods and tools:	NA
Responsibility:	Project manager.
Resources:	Project personnel, external resources as needed.
Exit criteria:	Selected actions have been implemented.

Table 24: The process definition information for the *risk control* process

Note that the risk control process can be initiated as soon as the first risk controlling action has been selected for implementation. Should the planning for all actions for all scenarios take longer, the implementation of selected actions does not, of course, need to be postponed.

6.7 Risk Monitoring

The *risk monitoring* process is a continuous process that monitors the status of the project and the status of risk monitoring metrics. The risk monitoring process is defined in Table 25. The risk monitoring process is initiated as soon as the actual work in the project starts. In practice, however, the process is activated after the first cycle of risk management has been carried out, as risk identification and risk analysis largely perform the functions of risk monitoring during the first cycle.

Although the risk monitoring process has been defined as a continuous process, in practice the project status and risk monitoring metrics are reviewed at some frequent intervals. This frequency is defined in the risk management mandate, but our experience indicates that weekly or biweekly reviews are normal. The time interval can be adjusted based on the risk management needs of the project.

Purpose:	Monitor the project and risk situation.
Description:	Continuously monitor risk monitoring metrics and the possible changes in project situation.
Entry criteria	Project has started. The process may be enacted on predefined frequencies.
Input:	Definitions for risk monitoring metrics. Risk management mandate. Goal definitions. Riskit analysis graphs.
Output:	Status reports.
Methods and tools:	Organization measurement program or database.
Responsibility:	Project manager.
Resources:	Project personnel.
Exit criteria:	Project has been concluded or terminated.

Table 25: The process definition information for the *risk monitoring* process

In practice the actual enactment of the process may take place in a project management meeting where some other issues are also discussed. However, we recommend that the risk monitoring activity is a dedicated activity that is consciously performed with care. If needed, the monitoring process can immediately lead to launching of risk identification or risk analysis processes as required in the same session, or separate session can be scheduled if necessary.

7. Conclusions

This document presented an operational definition of the Riskit method. To some degree the operational definition given here is perhaps too detailed for casual readers who want to read an overview of the method. Even practitioners may find the level of detail and the behavioral specification of the process too formal. However, we felt it necessary to provide such a complete and detailed definition so that the method itself is concretely and well defined. Without such a definition it is difficult, if not impossible, to evaluate the method. With the operational definition available, it can be used as a reference point between different organizations and project to compare their experiences and versions of the method.

We do recommend that this operational definition of the method is carefully reviewed and customized both in terms of content and level of detail before taking it into use in any organization. Such customization should take into account organizations' existing risk management practices, current risk management experience, available investment in risk management infrastructure, and desired level and rigor risk management. Our initial experiences indicate that the method itself is customizable. However, it is important to point out that attention should be given to the underlying principles of the method so that variants of the method do not become vulnerable to the many potential pitfalls common in risk management methods in industry.

We would also like to point out that additional information about the method and its usage experiences are available in separate reports and publications [19,29-31] and that additional information will become available.

We welcome all feedback and comments on the method and we recommend that method users contact Riskit method developers so that practical feedback from method use can be used to improve the method itself.

8. References

[1] Anonymous. *The American Heritage Dictionary of the English Language*, U.S.A.: Microsoft Bookshelf/Houghton Mifflin Company, 1992.

[2] Anonymous. *Merriam-Webster's Collegiate Dictionary*, Springfield, MA: Merriam-Webster, 1995.

[3] V.R. Basili, Software Development: A Paradigm for the Future pp. 471-485, 1989. Proceedings of the 13th Annual Computer Software and Applications Conference (COMPSAC). IEEE Computer Society Press. Washington, DC.

[4] V.R. Basili, Software Modeling and Measurement: The Goal/Question/Metric Paradigm CS-TR-2956, 1992. Computer Science Technical Report Series. University of Maryland. College Park, MD.

[5] V.R. Basili, G. Caldiera, F. McGarry, R. Pajerski, G. Page, and S. Waligora, The Software Engineering Laboratory - an Operational Software Experience Factory, pp. 370-381, 1992. Proceedings of the International Conference on Software Engineering, May 1992. IEEE Computer Society Press. Washington, DC.

[6] V.R. Basili, G. Caldiera, and H.D. Rombach. Goal Question Metric Paradigm. In: *Encyclopedia of Software Engineering*, ed. J.J. Marciniak. New York: John Wiley & Sons, 1994. pp. 528-532.

[7] V.R. Basili, G. Caldiera, and H.D. Rombach. The Experience Factory. In: *Encyclopedia of Software Engineering* , ed. J.J. Marciniak. New York: John Wiley & Sons, 1994. pp. 470-476.

[8] V.R. Basili, M.V. Zelkowitz, F. McGarry, J. Page, S. Waligora, and R. Pajerski, SEL's Software Process Improvement Program *IEEE Software*, vol. 12, pp. 83-87, 1995.

[9] A. Behforooz and F.J. Hudson. *Software Engineering Fundamentals*, New York: Oxford University Press, 1996.

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

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

[12] B.W. Boehm, Software Risk Management: Principles and Practices *IEEE Software*, vol. 8, pp. 32-41, 1991.

[13] M.J. Carr, S.L. Konda, I.A. Monarch, F.C. Ulrich, and C.F. Walker. *Taxonomy-Based Risk Identification*, SEI Technical Report SEI-93-TR-006, Pittsburgh, PA: Software Engineering Institute, 1993.

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

[15] R.N. Charette. *Applications Strategies for Risk Analysis*, New York: McGraw-Hill, 1990.

[16] R.N. Charette, Building Bridges over Intelligent Rivers *American Programmer*, pp. 2-9, September, 1992.

[17] B. Curtis, M.I. Kellner, and J. Over, Process Modeling *Communications of the ACM*, vol. 35, pp. 75-90, 1992.

[18] J.D. Edgar. Controlling Murphy: How to Budget for Program Risk (originally presented in Concepts, summer 1982, pages 60-73). In: Tutorial: Software Risk Management, ed. B.W. Boehm. Washington, D.C.: IEEE Computer Society Press, 1989. pp. 282-291.

[19] H. Englund, A Case Study to Explore Risk Management Methods 1997. Kunglika Tekniska Högskolan, Stockholm, Sweden. Masters thesis.

[20] R.E. Fairley. Risk Management: The Key to Successful Software Projects. In: *Proceedings of the 3rd IFAC/IFIP Workshop*, eds. F.J. Mowle and P.F. Elzer. Oxford: Pergamon, 1989. pp. 45-50.

[21] N.E. Fenton. *Software Metrics A Rigorous Approach*, London: Chapman & Hall, 1991.

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

[23] S. French. *Readings in Decision Analysis*, London: Chapman and Hall, 1989.

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

[25] D.W. Karolak. *Software Engineering Risk Management*, Washington, DC: IEEE, 1996.

[26] R.L. Keeney and H. Raiffa. *Decision with Multiple Objectives: Preferences and Value Tradeoffs*, New York: John Wiley & Sons, 1976.

[27] J. Kontio, Software Engineering Risk Management: A Technology Review Report PI_4.1, 1994. A proprietary Nokia Research Center project deliverable. Nokia Research Center. Helsinki, Finland.

[28] J. Kontio, *Promises*: A Framework for Utilizing Process Models in Process Asset Management, licentiate thesis at Helsinki University of Technology 1995.

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

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

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

[32] L. Laitinen, S. Kalliomäki, and K. Käsälä *Ohjelmistoprojektien Riskitekijät, Tutkimusselostus N:o L-4*, Helsinki: VTT, Tietojenkäsittelytekniikan Laboratorio, 1993.

[33] K.R. MacCrimmon and D.A. Wehrung. *Taking Risks*, New York: Free Press, 1986.

[34] M.W. Merkhofer, Quantifying Judgemental Uncertainty: Methodology, Experiences, and Insights *IEEE Transactions on Systems, Man, and Cybernetics*, vol. SMC-17, pp. 741-752, 1987.

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

[36] R.A. Radice, N.K. Roth, A.C. O'Hara, and W.A. Ciarfella, A Programming Process Architecture *IBM Systems Journal*, vol. 24, pp. 79-90, 1985.

[37] Rational, UML Notation Guide, version 1.1 1997. Rational Inc.

[38] J. Ropponen, Risk Management in Information System Development TR-3, 1993. Computer Science Reports. University of Jyväskylä, Department of Computer Science and Information Systems. Jyväskylä

[39] W.D. Rowe. *An Anatomy of Risk*, New York: John Wiley & Sons, 1977.

[40] T.L. Saaty. *Decision Making for Leaders*, Belmont, California: Lifetime Learning Publications, 1982.

[41] T.L. Saaty. *The Analytic Hierarchy Process*, New York: McGraw-Hill, 1990.

[42] H.A. Simon, Rational Decision Making in Business Organizations *The American Economic Review*, vol. 69, pp. 493-513, 1979.

[43] A. Tversky and D. Kahneman, Judgment under Uncertainty: Heuristics and Biases *Science*, vol. pp. 1124-1131, 1974.

[44] Visio Corp., VISIO Technical, ver. 4.0, rel. 1995. Visio Corporation. IBM compatible PC. MS-Windows, Windows 95.

[45] J. Von Neumann and O. Morgenstern. *Theory of Games and Economic Behavior*, Princeton: Princeton University Press, 1944.

[46] E. Yourdon. *Decline and Fall of the American Programmer*, Upper Saddle River, NJ: Prentice-Hall, 1992.