AN OVERVIEW OF SOFTWARE RISK MANAGEMENT METHODS*

Calvo-Manzano,J.A.; Maté J. L.; San Feliu, T.
Departamento Lenguajes y Sistemas Informáticos e Ingeniería del Software.
Facultad de Informática. Universidad Politécnica de Madrid

Software projects have often suffered in the past from alarming overruns of the budget and schedule, due mainly to the uncertainty of the development schedules and costs estimations. In responding to such question the software industry has gained a great deal of experience in techniques for risk management. More interesting risk management methods are shown. A brief summarize description of the four major methods, its risk definition, phase description and principal characteristics with the relative strengths and weakness of each method is given.

Keywords: Software management, software engineering, risk management, risk assessment, risk analysis.

1. INTRODUCTION

Most organizations are highly dependent on information systems that stand on software and another forms of automatic support. Staying in a competitive environment, which leads to an increasing complexity of the systems to develop, means to arrange a higher degree of automatic support. Yet we must often deal with the following problems: schedule or budget overruns, systems that do not come up to user expectations, money continuing to be spent on completing projects even after it is apparent that the system is defective or is no longer a cost-effective project or systems that work but do not contribute to the organization's goals.

Therefore the risk management area has been expanding over the past years [1]. Why so much concern? One possible answer is: the complexity of software systems is on the increase, and there is a higher interest in a higher quality. Nevertheless it is not a matter of eliminating each and every risk human activity, the goal is not to get risk free technologies, but to determine whether the levels at which we can state are safe enough and the benefits of the activities can overcome possible damages.

When developing a project most analysis of failures show that problems could have been reduced or even solved, if there had been an explicit early concern with to identifying and resolving risk elements. Usually there is excessive optimism during the early phases of the project which lead some clear signs indicating a high risk situation being dismissed.

Modern methods of development make it all too easy for project managers to make high risk agreements they may regret in the future. Sequential life cycle models [2] driven-document like the waterfall model do not provide for the high risk implications arising from the requirements to be established when the contract is made. Experience has shown that successful project managers are good risk managers, although they do not use terms such as risk identification, risk evaluation and planning, however this is precisely what

they are doing. And their projects tend to overcome obstacles and produce good products. This has led to an effort to formalize the applied mechanisms as a "Software Risk Management" discipline.

2. BASIC PRINCIPLES IN RISK MANAGEMENT

We define project risk as the sum of factors that prevent the system from being delivered, meeting the user's requirements or being delivered within a stated time and a previously fixed budget. But this is not the only definition of risk, different authors on risk management methodologies will suggest definitions according to any aspect they want to consider, so risk is defined as "the probability of an undesired event and its impact"[3], or "risk is the traditional manner of expressing uncertainty in the system's life cycle. In a quantitative sense, risk is the probability, at a given point in a system's life cycle, that predicted goals cannot be achieved with the available resources"[4]

Formally, risk is represented by the triplet [5] $<s_i,l_i,x_i>$, where "s" contains the scenarios on what can go wrong, "l" represents the generic likelihood associated to the scenarios and "x" represents the measure of the possible consequences. In order to identify risk areas, we need a classification of risks, whether by their origin, or the point they manifest, or the impact they produce on development. Thereafter, possible couplings and dependences between risk elements must be studied.

Risk management is making informed decisions by consciously assessing what can go wrong and the resulting impact. Risk management is accomplished by a continuous set of activities to identify, confront and resolve risks [6].

The principal phases of each software risk management process are the following:

- Identification. In this phase, potential risk items must be investigated and extracted, as well as their sources, estimations of the associated probability and its effects during a given period. The purpose of these studies is to establish a justification of the costs, in order to select and introduce preventive measures. Risk identification must be done by means of a structural and disciplinary process, in order to identify and analyse systematically the risks.
- Planning. In this phase the information obtained is transformed into decisions and actions (both present and future). Consideration is required to determine: (a) how often monitoring should be performed; (b) by whom; (c) how extensive it should be; and, (d) at what time, and at what level should be the new risk state be set?
- Monitoring. In this phase deviations from planned actions, the behaviour of risks and the appearence of new ones are controlled. Periodic application of risk monitoring is required to judge progress in averting the currently known risks, and to surface any unobservable risks. Results of the monitoring effort should be used to determine the effectiveness of the risk handling techniques.

3. CURRENT METHODS

This paper presents a comparison of the most current important methodologies on risk management today, according to the following scheme for each one: risk definition, phases description and its principal characteristics with the relative strengths and weakness.

- Portfolio Approach to Information Systems.
- Software Risk Abatement.
- Method of Charette.
- Method of Böehm.

3.1. Portfolio Approach to Information Systems

Proposed by McFarlan in 1981, [7] this method identifies risks, provides possible techniques for their resolution, and bases the identification phase on a classification of the organization and its projects.

3.1.1. Risk definition

According to the author, risk means what is left after having applied appropiate managing methods and techniques.

It is distinguished the following risk consequences:

- Failure to obtain all or part of the expected benefits.
- Implementation costs exceed the accepted values.
- Implementation takes longer than expected.
- Technical performance of the systems is lower than expected.
- Incompatiblity of the system with the selected hardware and software.

The author proposes three risk dimensions:

- Project size. Size affects cost, staffing levels, passed time and number of departments the project involves.
- Experience in technology: Due to a higher probability of dealing with unexpected technical problems, the project's risk increases according to the previous experience in hardware, operating system, database management systems and project application language.
- Project structure: In some projects, the very nature of the task is defined at the moment of conceptualization, which provides structural schemes. These are processes that will not be modified during the project's life cycle.

3.1.2. Phase description

The primary steps are:

- Identifying the category of the project among different categories, according to the three dimensions, each one indicating a different degree of risk. It is useful to categorize projects when separating them into their management forms. Risk measurement aims to do this by considering questionnaires developed on the basis of experience in successful or failed projects. The answers to the questions not only make projects

clear, but also suggest alternative ways of project management. If the risk scoring is high, an analysis of the answers may come up with ways of handling risks. At this point, managers must not consider risk as static; moreover, its presence must encourage a better focus better on management.

- Risk control: When, as a result of the previous step, a high scoring is determined, this must be approved by the manager, because this is the way to make sure that managers notice risks and make an assess the consequent benefits. In addition, the aggregate risk of other projects must be determined.
- Project monitoring is done in accordance with planning and control tools. What kind of tools and techniques must be used? These are established depending on the organization and complexity of the project.

3.1.3 Principal characteristics

This method focuses on risk taxonomy, that is the three risk dimensions of a project (size, experience, and structure). Another point of interest is the emphasis on what types of management tools and approaches must be applied to ensure project success.

This approach is focused on personal experiences, coupled with other learning experiences and knowledge of the organization's mission. Risk factors must be at least partially identified from checklists in order to get easyly the information needed for the decision process, because actually the only parameter of the decison process is the risk score. Unlike rest methods, the coverage of all life cycle is not contemplated in this approach.

3.2. Software Risk Abatement. AFSC-800-45

The U.S. Air Force has since been a pioneer in the development and application of risk management techniques. This document summarizes its current approach. The risk management process is an iterative process that requires goals established by the managers, who will regularly evaluate the impediments to achieving these objectives. Risk management must be considered from the point of view of the magnitude of causes and effects of changes.

3.2.1. Risk definition

Risk is the traditional manner of expressing uncertainty in the system's life cycle. In a quantitative sense, risk is the probability at a given point in a system's life cycle that predicted goals cannot be achieved with the available resources[4]. Software risks can be divided into: risk in the performance, support, costs and planning.

3.2.2. Phases description

The software risk management process is divided into:

- Identifying risk components
- Analysing risk factors
- Developing options for dealing with risk and controlling risk factors

- Risk identification. Before starting the process, it is necessary to determine whether software contributes meaningfully to the total risk in the system. Next, risk elements are identified and, at this point, we can obtain information from historic data of similar programs, lessons learned, previous research and precise

studies on similar development programs. Risk items will be identified by analysing these data, as well as its impact on the system.

- Risk components analysis. The analysis of each risk component in the system must be done using techniques from multiple disciplines in order to determine the probability of a risk item and its impact. Impact is divided into four categories: catastrophic, critical, marginal, negligible. Categories are determined by the potential consequences of possible undesired results due to undetected software errors or faults. After the impact and probability of occurrence have been evaluated, the degree of risk can be determined. The seriousness of risks is subdivided into: high, moderate, low or none.
- Management and control of risk. This task manipulates risk factors so that the exposition to risk can be reduced. Risk handling alternatives are divided into four categories: avoidance, control (prevention), assumption and transfer. The selected technique depends on the part of a program where the project falls and on the possible avaible options. After having selected the risk management technique, the results of this technique will be compared with expected ones in order to determine the need of continue with or take possible actions, repeting them when necessary.

3.2.3 Principal characteristics

This method provides a set of guidelines for applying risk management, mainly based on previous USAF experience. Several set of tables for risk identification and risk assessment are given, in order to facilitate the estimation of risk items.

The principal weakness of this approach is that it has been designed in a specifically military environment, however it gives a good set of guidelines for use in a software risk team.

3.3. Method of Charette

3.3.1. Risk definition

Charette defines risk [5] as any event, happening or thing that has a loss associated with it or uncertainty or some choice is involved. The primary sources of risks are lack of recognition or appreciation of risks, lack of the necessary resources, and, lack of productivity of the resources.

3.3.2. Phases description

Charette divides the method for software risk management into two major phases: risk analysis and risk management.

- Risk Analysis. It is the process of identification, estimation and evaluation of risks. Risk analysis is used to identify potential problem areas, quantify risk associated with these problems and generate alternative courses of action that can be taken to resolve risk.

1. Risk identification: Before making risk analysis, it must be considered whether the analysis is necessary. Risk identification is the comprehensive identification of potential risk items using a structured and consistent method, obtaining at the end of this step a categorized list of risks.

2. Risk estimation consists in measuring the probability of potential loss and to risk exposure; during the estimation process the measurement scale will be selected, so that quantitative data about risks can be obtained, trying to reduce the uncertainty of risk estimations.
3. Risk evaluation is a process that makes it possible to foresee answers to risks. The purpose is to foresee the consequences of the different possible alternatives, comparing them with the acceptability of individually predicted consequences to a foreseen decision.

- Risk Management is the planned control of risks and the monitoring of the success of the control mechanisms. Risk management involves making a risk analysis and taking a decision. Three tasks are required to perform risk management.

1. Risk planning. Risk planning is concerned with two principal questions: first, whether the strategy that will be applied for managing risks is feasible and correct; and second, whether the tactics and the means available to implement this strategy fit in with the project's goals.
2. Risk control. Risk control involves the development and evaluation of the feasibility of the implementation of the plan's control mechanisms for the reduction strategies. A control of any contingency that should be in reserve must be established. A risk management plan will be draw up, determining one possible strategy against risks: reduction, protection, transfer, pecuniaries.
3. Risk monitoring. Monitoring comes after the decisions on the reduction strategy and tactics have been already implemented in order to avoid possible risk, that is:
    - Check if the consequences of the decision were the same as foreseen.
    - Identify opportunities for refining of the risk aversion plan.
    - Provide feedback for future decisions concerning the control of new risks or current risks that do not respond to risk aversion, or risks whose nature has changed with time.

3.3.3. Principal characteristics

- This methodology provides severals mechanisms for categorizing risks.
- It also generates a complete documentation: a risk estimation situation document for risk identification and a software risk management plan and software risk aversion plan for risk planning and monitoring phases.

3.4. Method of Böehm

Böehm's software risk management [3] approach of 1989 is based on experience in TRW projects.

3.4.1. Risk definition

Risk is the possibility of loss or injury. This definition can be translated into the concept of exposure to risk, which relates the two basics of risk, probability and possible potential loss. These are factors that will determine possible alternatives to reduce risks, by minimizing probability or impact or both of them.

3.4.2. Phases Description

Risk management practice involves two primary phases and each one with three subsidiary steps.

The first phase, risk assessment, involves risk identification, risk analysis and risk prioritization.

- Risk identification produces lists of the project-specific risk items likely to compromise a project's success. The most common techniques of identification include checklists, examination of decision drivers, comparison with experience and decomposition.
- Risk analysis assesses loss probability and loss magnitude for each identified risk item, and it assesses compound risk in risk-item interaction. The most common techniques are: perfomance models, cost models, network analysis, statistical decision analysis and quality-factor analysis.
- Risk prioritization produces a ranked ordering of the list items identified and analysed risk items. Typical techniques include risk-exposure analysis, risk-reduction leverage analysis, Delphi or group-consensus techniques.

The second phase in risk control involves risk management planning, risk resolution and risk monitoring.

- Risk management planning helps to prepare the strategy for each risk item, including the coordination of the individual risk item plans with each other and with the overall project plan. Most common techniques include checklists of risk-resolution techniques, cost-benefit analysis, and standard risk-management plan outlines, forms and elements.
- Risk resolution produces a situation in which the risk items are eliminated or, at least, reduced. Typical techniques include prototypes, simulations, benchmarks.
- Risk monitoring involves tracking the project's progress toward resolving each risk item and taking corrective action where appropriate. The most common techniques includes milestones tracking, top-ten risk item list, that is reviewed weekly or monthly, followed by reassessment of the risk item, or corrective action.

3.4.3 Principal characteristics

This approach provides a well-defined set of stages, with a well assembled collection of techniques, tools and forms to use in risk management. This framework is flexible to use with several life cycle models, specially designed for the spiral life cycle model [8].

Böehm and Charette's methods focus on similar points of interest:

- Improve qualitative assessment through documentation and reviews.
- Prevention of risk by using highly experienced personnel.

While Böehm's approach works on a unique document (risk management plan) refined by iterative reviews, Charette's approach provides a very different structured documentation, it establishes a document (risk estimation situation) to use in the risk identification phase and two more documents to use in the planning phase (risk management plan and risk aversion plan).

4. SUMMARY

The different methodologies we have presented provide a framework where risk management can be applied in practice. They do not pretend to be the philosopher's stone, nor making success completely sure; nevertheless they are important, because they can help avoiding disasters by focusing on the critical factors of success. There are still points to determine, since risk management needs human judgement on technical and personal factors. In the future, risk management will basically progress in two areas: first, on the new ways of getting software develop process, and, second, on the improvements of risk management techniques. As regards the former, a great effort is being made at the Software Engineering Institute[9] to come up with a process for evaluating software capabilities. Research on the latter is already underway with a view to incorporating new artificial intelligence techniques and fuzzy logic in order to help overcome problems with risk quantification techniques, which will may it possible to improve existing methods. So we must introduce the future changes in improving techniques arising from the experience in applying risk management in more number of projects, and provide a support in the shape of integrated control tools that facilitate an automatic capture of information, filtering and exploring possibles alternatives and solutions to make decisions easier. This work is being carried out in Europe by the EUREKA RISKMAN Project, and in the United States by the System Engineering Risk Management Institute and Software Engineering Institute at Carnegie Mellon.

REFERENCES

[1] M. G. Morgan, "Choosing & Managing Technology-Induced Risk", IEEE Spectrum, Dec 1981

[2] A.M. Davis, E.H. Bersoff, E.R. Comer., "A Strategy for Comparing Alternative Software Development Life Cycle Models", IEEE Transactions on Software Engineering, Oct 1988

[3] B. W. Böehm.Software Risk Management Tutorial. IEEE Computer Society, 1989

[4] U.S. Air Force Systems Command, Software RiskAbatement, AFSC Phamphlet 800-45,1988

[5] R. N. Charette, Software Engineering Risk Analysis and Management", McGraw-Hill 1989.

[6] Department of Defense, Software Technology Strategy, Draft December 1991.

[7] F. W. McFarlan, "Portfolio Approach to Information Systems", Harvard Bussiness Review, Sep-Oct 1981.

[8] J. G. Wolff, "The Management of Risk in System Development: 'Project SP' and the 'New Spiral Model', Software Engineering Journal, May 1989

[9] W.S. Humphrey, "A Method for Assessing the Software Engineering Capability of Contractors", CMU Software Engineering Institute Report CMU/SEI-87-TR23 Carnegie Mellon Univ. Press, 1987