IMPLEMENTING AND IMPROVING THE SEI RISK MANAGEMENT METHOD IN A UNIVERSITY SOFTWARE PROJECT

IE Working Paper SI8-109-I 19-10-2004

José Esteves
Instituto de Empresa
Madrid, Spain
Jose.Esteves@ie.edu

Joan Pastor
Univ. Int. de Catalunya
Barcelona, Spain
jap@unica.edu

Núria Rodriguez
Univ. Polit. de Catalunya
Barcelona, Spain
nuria.Rodríguez-camara@upc.es

Ramon Roy
Univ. Polit. de Catalunya
Barcelona, Spain
ramon.roy-torras@upc.es

Abstract

Although risk manag ement approaches appeared more than one decade ago, there is the evidence of low pe netration rate of their techniques in software projects. One of the most widely known methods is the SEI Software Continuous Risk Management (SEI-CRM) method. This pape r addresses the usage of the SEI-CRM method in a big software development project. The study we carried out sug gests that SEI -CRM is limited in terms of the organizational risk perspective. This research i s expected to contribute with the knowledg e on risk manag ement for software development projects by for which we propose to ex tend the SEI-CRM method with some organizational risk factors that we have found relevant from our study.

Keywords

Risk management methods, SEI-CRM method, organizational risks

1 INTRODUCTION

Software Risk Management research is a task that attempts to formalize risk-oriented correlates of development success into a readily applicable set of principles and practices (2000). Several risk management approaches have been proposed and used since Boehm (1988) brought risk management to the attention of the software engineering community. However, there is the evidence that few organizations use specific methods for risk management systematically [10,11]. KLCI (2001) (2001) conducted a study in 268 organizations worldwide and it found that 3% did not used any risk approach, 18% used an ad-hoc approach to identify their risks, 37% of the participants used an informal approach, 28% use repeatable procedures (periodic approach), and only 14% used a formal approach to identify their risks. The common reasons for using an informal approach include: lack of procedure, adequately meet projects needs, young/immature organization, and team focus. According to Hoffman (1998), even those organizations that use formal risk management processes for other parts of their business demonstrate consistently poor Information Systems (IS) risk management and take a fragmented approach to it. Kontio and Basili (1997) believe that there are three primary reasons for the low penetration rate of risk management technology: lack of knowledge about possible risk management methods and tools, practical and theoretical limitations of risk management approaches that hinder the usability of these methods, and third, there are few reports on systematic and scientifically sound evaluations to provide empirical feedback on their feasibility and benefits.

Software project risk includes technical and behavioral risk components (2001). Different studies have shown that most projects fail managerially, not technologically. Organizational issues are the most dominant project risk factors, but they are satisfactorily treated in less than a third of systems development projects (2001). Schmidt et al. (2001) found that successful project managers rank low those factors over which they have no control or influence such as: conflict between user departments, change in ownership or senior management, staffing volatility, number of organizational units involved, and multi-vendor projects. Another aspect is the lack of recognition within the IT community about the importance of organizational issues as evidenced by Doherty and King (2001). The purpose of this paper is twofold. First, we attempt to describe the usage of the SEI CRM method in a big software development project. Second, to extend the SEICRM risk taxonomy with organizational risks based on the unified model of critical success factors for Enterprise Resource Planning (ERP) implementations proposed by Esteves and Pastor (2000). Thus, the risk identification strategy proposed in this paper has some innovation when compared with other related work. There are two main reasons to adopt the ERP unified model. First, the same organization implemented an ERP system two years before the start of the mentioned software development project. We suggest that the information related to the predicted or occurred risks in former organization projects (such as their causes, consequences, their treatment and success of the mitigation and contingency actions) may help managers identify and manage new project risks. Besides, lessons learned regarding risk management for former projects might contribute to the enrichment of the project risk planning approach. Second, the ERP unified model includes a well defined and concise model of organizational critical success factors which may easily be reinterpreted as “critical risk factors”.

This paper is structured as follows. First, we describe the background of this study. Then, we describe the risk management phases. Next we present the risk method implementation for our case study. Then, we explain the extension of SEI CRM risks. Finally, we present the implications and further work.

2 THE PRISMA PROJECT BACKGROUND

The Universitat Politècnica de Catalunya (UPC) of our study is a Spanish higher education institution whose priority goals are teaching, research and technology transfer. UPC was created in the 70s and it is composed of 15 academic schools, 7 associated schools and 3 academic institutes with more than 30.000 students. One of its main purposes is to transfer its academic results to industry. In this sense, it is the most important Spanish university in terms of resources obtained from research based on the technology transfer with companies.
UPC has had different several software packages for the management and administration of the studies of the university. After some evaluations in the market alternatives the UPC took the decision to develop its own new IS for administration of the academic studies, and selected an internal IT unit to develop it. The project was called PRISMA, and its three main goals were to build one single IS for academic information, provide multi-channel access to the academic IS (school, Internet, mobile) and support the adaptation to the "Bologna Declaration", or convergence of European academic studies.

3 PRISMA RISK MANAGEMENT PHASES

3.1 Identification and selection of a risk management approach

This phase consisted in the identification and the evaluation of the alternative risk management approaches for implementing the fundamental risk management functions that must be taken to effectively manage risks before they become threats to success or major sources of rework. Table 1 shows the risk methods evaluated: Euromethod, Safe, SEICRM, IEEE, RiskIt, Project Management Institute (PMI) risk method. We would like to note that each method categorized the risk functions in different phases. For each method we analyzed what and how each one of the functions in table 1 was implemented.

<Introduce Table n. 1 here>

The risk management team and the project manager decided to adopt the SEI CRM method due to two main reasons. First, SEICRM is one of the most complete risk methods with detailed documentation which is applied in industry. Second, the PRISMA project also started implementing the Capability Maturity Model (CMM) level 2 from the SEI, which helped to incorporate SEICRM as part of the tasks of CMM level 2.

3.2 The SEICRM Method

This section describes the SEI Continuous Risk Management (SEICRM) method, developed by the Software Engineering Institute (SEI), is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to: assess continuously what can go wrong (risks), determine what risks are important to deal with, and implement strategies to deal with those risks. When using CRM, risks are assessed continuously and used for decision-making in all phases of a project. Risks are carried forward and dealt with until they are resolved or they turn into problems and are handled as such. Table 1 shows the typical risk functions. The SEI CRM has a similar set of functions, but also includes the notion of performing tasks on a cyclical basis, that is: identifying, analyzing, planning, tracking, controlling and communicating the risks throughout a project life cycle.

3.3 Definition of PRISMA Risk Management Plan

Our first task was to create a project risk management plan. Although the SEICRM method does not include a specific phase or task to develop the risk management plan, we opted to extend SEICRM phases with the PMI risk management plan definition phase. The purpose of this plan was to guarantee that the PRISMA project risks were identified, analyzed, documented, mitigated, and controlled in a correct way along the project life cycle. The project risk management plan specifies the processes, methods, responsibilities and tools associated with risk management in PRISMA and follows the SEI SWCMM and the PMI recommendations.

3.4 Definition of the RISK MANAGEMENT Team

Figure 1 depicts the responsibilities of all project personnel including project manager, software technical managers, team members, and risk management team for managing risk within the PRISMA Project.

<Introduce Figure n. 1 here>

The main responsibilities for each risk role were:

- Team members: identify new risks, estimate probability and impact, classify risks, recommend actions, track risks and mitigation plans, and assist in risk prioritizing.
- Technical managers: integrate risk information from all individuals within their department, ensure accuracy of probability and impact estimates and the classification, reprioritize all risks to determine high importance risks, review recommendations on mitigation actions, assign or change responsibility for risks and mitigation plans, report to the project manager, implement control decisions for risks, build action plans, collect and report general risk measures, and coordinate communications with the project manager.
- Project manager: authorize resources for mitigation, integrate risk information from all managers, reprioritize all risks to determine high importance risks, make decisions to control these risks, assign or change responsibility for risks and mitigation plans within the project, and review measures with quality department periodically to evaluate effectiveness.
- Risk management Team (Quality team): coordinate activities to identify and analyze risks, maintain the project risks list, notify new risks and report periodically risks status to the project manager.
- Team to support the risk management team: detect risk elements and estimate potential negative impact, review and evaluate critic processes and dept within the project, review and import relevant results from other similar internal or external projects, build policies and contingency plans, and assess and assist the project manager in high critic activities.

4 PRISMA SEICRM IMPLEMENTATION

4.1 Risk Identification Phase

The risk identification phase consists in activities and methods used to discover risk factors before they become problems. The risk identification process followed in PRISMA is shown in figure 2 and it was divided in two phases: identification of an initial list of project risks and continuous risk process management.

<Introduce Figure n. 2 here>

1. Identification of an initial list of project risks

The risk manag ement team built a risk identification questionnaire based in the SEI risk taxonomy. The tax onomy provides a framework for identifying technical and programmatic software development risks (1993). The SEI taxonomy contains 194 questions org anized into three major classes: product eng ineering, development environment and program constraints. Some authors (e.g . (1997)) have stressed that the SEI taxonomy seems desig ned to better support risk identification for larger, more formaliz ed, and more technical projects for larg e organizations. The down side of the current taxonomy is that it reflects its orig ins, that is, that the types of risks encountered are those that ex ist typically in large often military organizations undertaking very large software development projects. W e extended this taxonomy by defining another class, org anizational risk factors, imported and adapted from the organizational and strategic factors identified by Esteves and Pastor (2000) for ERP systems implementation (see table 2).

<Introduce Table n. 2 here>

In the view of Esteves and Pastor (2000), the nature of the ERP implementation problems includes strategic, tactical, organizational and technolog ical perspectives. Then, we proposed that the critical success factors unified model should have these four perspectives. The organizational perspective is related with concerns like org anizational structure and culture, and business processes. The strategic perspective is related with core com petencies accomplishing the organization's mission and l ong-term goals, while the tactical perspective

affects the business activities with short-term objectives. The risk manag ement support team used this questionnaire as the basis to conduct interviews with manag ers in order to elicit risks. Moreover, information about risk manag ement on similar projects within the organization and from outside was studied to perform the analysis and to make the provisional list of project risks. As a result of comparing this list with other risk checklists, the initial list of project risks was built.

2. Continuous Risk Process Management

All the PRISMA project team members are responsible for identify ing new risks during the whole project lifecycle. See below for more details on continuous risk process management.

4.2 Risk Analysis Phase

The purpose of the risk analysis phase is to convert the risk data into decision-making information. This involves establishing values for impact (the loss or neg ative effect on the project should the risk occur); and probability (the likelihood the risk will occur). The process of analyzing risks has three steps: evaluating the attributes of the risk; estimating probability and impact using a five score scale, ensuring accuracy of risk attributes; and classifying and prioritizing the risks.

4.3 Risk Plan Phase

Taking the prioritized risk list as input, the risk plan activity consists in deciding what to do and when, if any thing should be done about a risk. I n this phase decisions and mitigation strategies are developed based on current knowledge about project risks. The risk strateg y for a specific risk can take many forms: Transfer, mitig ate, avoid, and accept the risk. In this phase we only considered allocated planning resources and mitigation activities for risks with high or moderate importance. The risk plan process has the nex t steps: assig nment of risk responsibility to any project stakeholder; creation of an action plan for each risk, if the action opted is mitigation, then a mitigation plan should be created; and revision of all action plans.

4.4 Risk Tracking Phase

Tracking is a process in which risk data are acquired, compiled and reported by the person(s) responsible for tracking watched and mitigated risks. Key performance indicators are gathered and presented to decision-makers in tracking documents and/or presentations. This phase involved the following steps: monitor risk indication and mitig ation plans, new risks identification, prioritized risks list.

4.5 Risk Control Phase

The purpose of this phase is to correct for deviations from the risk mitigation plans. In addition to monitoring the risks on its current list, the team needs to be alert to new risks that enter its environment as the project proceeds. This process is composed of the following steps: identification of a new project risk, submission of risk proposal, risk confirmation, assignment of someone responsible for the new risk, and periodical revision of new project risks.

4.6 Communication Phase

The purpose of the communication phase is to provide information and feedback to and from the project on the risk activities, current risks, and emerging risks. Communication is essential to the success of all other functions and is critical for manag ing risks. For effective risk management, an org anization must have continuous and open communication. It occurs formally as well as informally. We carried out the following activities: presentations and workshops of risk management approaches to the PRISMA team members, publicize the list of risks, and report periodically the status of project risks to software technical managers, project managers and the steering committee. All risk documents are accessible online in a risk management tool (a lotus notes application).

5 ORGANIZATIONAL RISK FACTORS IN THE PRISMA PROJECT

Table 3 shows the risks factors identified in the PRISMA project which were initially incorporated from the Esteves and Pastor (2000) model. We would like to note that the risks titles do not match ex actly with Esteves and Pastor (2000) factors because these factors were

defined as categories defined in a higher level than our risk factors, and because success factors were reinterpreted as risk factors.

<Introduce Table n. 3 here>

Next, we briefly discuss some of the organizational risks identified and the actions taken for each organizational risk.

5.1 Lack of an organizational change management plan

This organizational risk was classified as a risk with high importance. This status is similar to the literature on risk management that suggests that the risks associated to the change of culture are the most difficult to manage (1990). Culture is normally the most powerful force opposing change and the implementation of cultural change is a long term process which needs to be managed carefully. For this risk, the PRISMA risk management support team defined the following mitigation action: develop effective communication between the project management team members including steering committee and the stakeholders who must change or play a key role in the change process.

5.2 Lack of user involvement and participation

User participation refers to the behavior and activities that users perform during the system implementation process. User involvement refers to a psychological state of the individual, and is defined as the importance and personal relevance of a system to a user (1994). User involvement and participation will result in a better fit of user requirements achieving better system quality, use and acceptance. With regard to the mitigation of this risk, we developed a set of activities to improve user involvement especially in critical tasks such as training and system implementation.

5.3 Lack of inwards and outwards communication

According to Esteves and Pastor (2000), communication should be of two kinds: 'inwards' the project team and 'outwards' to the whole organization. This means not only sharing information between the project team but also communicating to the whole organization the

results and the goals in each implementation stage. There is the need to create a communication plan to organize all the communication tasks. Furthermore, the communication effort should be done in a regular basis during the implementation phase. For this risk, the PRISMA risk management team defined the following mitigation actions: we proposed to create a communication plan. The communication plan determined the information and communication needs of the stakeholders: who needs what information, when they will need it, how it will be given to them and by whom. We proposed to perform more frequent and regular meetings (all project team and only software technical managers).

5.4 Inadequate training program planning and assessment

The purpose of training is to develop the skills and knowledge of individuals so they can perform their roles effectively and efficiently. We considered not only evaluating and monitoring training for PRISMA team members but also for the users of the system. Concerning users one of the most important benefits on evaluating training is that it serves to adapt users to the new system, thus helping the organizational change process. For this risk, the PRISMA risk management team defined the following mitigation actions: create a training plan which documents the objectives of the training program, the training needs, the training to be delivered and tactical procedures for carrying out training activities; provide a set of metrics to control the training in PRISMA, using a framework proposal for monitoring and evaluating training in ERP implementation projects; create a training evaluation questionnaire; collect the data using surveys that the users or the PRISMA team members respond each time they take a course; analyze the data to determine the status of the training plan and propose training improvements.

6 DISCUSSION AND FURTHER WORK

Two relevant findings have emerged in this study . First, the applicability of SEICRM approach. Overall, the people that participated in the risk management process agree that SEICRM is a positive process. However, based on our experience in this project we think that one of the main problems of SEI CRM method is that it presumes a level of software project management planning maturity of the organization that may be difficult to find in many projects. Another issue that may affect the SEICRM applicability is implied by the

misconceptions surrounding the application of any risk management approach. Padayachee (2002) mentions that misconceptions arise "through viewing risk management as being implicit in the planning or specification phase or viewing risk as challenges, therefore negating the need for a risk management". This attitude may affect the involvement and participation of risk evaluators in the whole process. Managers can accept easily their participation in the risk identification phase. Our experience shows that the SEICRM taxonomy questionnaire needs to be adapted to the specific context of each software development project. A good software project manager cannot afford that his software technical managers are wasting their time in answering reports with questions not fitting with their project. Thus, the use of the standard SEI CRM questionnaire may decrease the level of confidence in the risk identification process and in the risk management team work.

We also think that conducting interviews with software technical managers helped to improve the risk data collected since the information of interviews information was more detailed. This aspect confirms Kontio et al. (1998) analysis that information gained in interviews was more detailed and of better quality than the results of workshops, perhaps due to more confidential nature of interviews and the possibility to focus on specific topics. The risk analysis phase seems quite well accepted by managers. While the risk identification and analysis phases begun at the same time of the software project development, the other risk phases started when the software technical managers were concentrated resolving schedule and budget problems and reducing their effort on the activities to ensure quality control like risk management. Thus, there is not a mitigation action plan for each risk that is to be mitigated and not all the contingency plans have been documented. Concerning tracking and control phase, the situation is similar so we suggested that the risk management team has to communicate, motive and help the software technical managers to plan each risk to be mitigated and track and control it.

The second finding is related with the extension of the SEI taxonomy with organizational risks, and the other is the level of importance of these organizational risks perceived by the project manager and software technical managers. The risk evaluators identified almost all the organizational risks as with medium importance. Most of these risks were not under the direct control of the project manager or of the software technical managers. This finding is supported by other risk management studies (e.g. (1998)) that have shown that most of the risk lists focused on those risks factors over which the project manager has a relatively degree

of control. The risk evaluators also did not consider some organizational issues as risks because they could not effectively control them or they analyzed the organizational issues as related with their own role. For instance, software technical managers did not consider low empowerment of decision-makers as a risk because they analyzed this issue in relation to their role and not their subordinates. Overall, we detected that the emergence of organizational issues related with people roles and skills is very difficult since people may avoid admit explicitly that they or the others may not act as expected. We think that the main reason is to avoid conflicts among evaluators. We also think that software project risk management in terms of organizational perspectives requires a comprehensive knowledge of previous experiences acquired in previous projects. Since the researchers within the risk management team conducted a case study of the critical success factors in the previous ERP implementation in the organization, they contributed with some project risks. Based on this previous experience it was also possible to avoid and mitigate some of those problems that occurred in the ERP implementation in a more adequately manner. This experience also helped to incorporate some valuable solutions found in the ERP implementation (e.g. the training program monitoring). We think that organizations would benefit in the creation of a risk management database for their different projects since it would help managers identify and manage new project risks. Our experience suggests that technical risks have a solution that in most cases depends mostly on the cost and the availability of the technology required while organizational risks go beyond the project boundaries. In this project, we have seen that managers were able to contextualize and adapt the SEI CRM method to their needs. As with other IS development methodologies, techniques and tools, risk management approaches adoption should be treated with caution.

7 REFERENCES

Adler, P., & Shenhar, A. (1990). Adapting your technological base: the organizational challenge. Sloan management review, 25-37.

Boehm, B. (1988). A Spiral Model of Software Development and Enhancement. IEEE Computer, 21, (1988) 61-72.

Carr M., Konda S., Monarch I., Ulrich F., & Walker C. (1993). Taxonomy-Based Risk Identification. Technical Report CMU/SEI-93-TR-6, Software Engineering Institute, Carnegie Mellon University.

Doherty N., & King, M. (2001). An investigation of the factors affecting the successful treatment of organizational issues in systems development projects, European journal of information systems, 10, 147-160.

Esteves J., & Pastor J. (1999). Towards the Unification of Critical Success Factors for ERP implementations, 10th Annual BIT conference, Manchester, UK.

Hartwick J., & Barki (1994). Explaining the Role of User Participation in Information System Use. Management Science, 40(4), 440-465

Hoffman T. (1998). Risk management still a wild frontier, Computerworld, 32(7), 10.

Jiang, J., Klein, G., & Discenza, R. (2001). Information Systems Success as impacted by risks and development strategies. IEEE transactions on Engineering Management, 48(1), 46-55.

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

KLCI (2001). Software Risk management Practices – 2001. KLCI research group report, http://www.klci.com (2001)

Kontio, J. (1997). Empirical Evaluation of a risk management Method. SEI conference on risk management, USA.

Kontio, J. Getto, G., & Landes, D. (1998). Experiences in improving risk management processes using the concepts of the Riskit method, SIGSOFT'98 sixth international symposium on the foundations of software engineering.

Mitchell T. (1997). Matching Motivational Intervention to Organizational Contexts. Research in Organizational Behavior, 19, 57-149.

Moynihan T. (1997). How Experienced Project Managers Assess Risk. IEEE software, 35-41.

Padayachee K. (2002). An Interpretive Study of Software risk manag ement Perspectives. South African I nstitute for Computer Scientists and Information Technologists (SAICIST) conference, 118-127.

Roppponen, J., & Lyytinen, K. (2000). Components of Software Development Risk: Hot to address Them? IEEE transactions on software engineering, 26(2), 98-111.

Schmidt, R., L yytinen K., Keil M., & Cule P. (2001). I dentifying software project risks, an international Delphi study. Journal of management information systems, 17(4), 5-36.

Walsh K., & Schneider H.(2002). The role of motivation and risk behavior in software development success, Information research, 7(3), [Available at http://InformationR.net/ir/7-3/paper129.html].

8 FIGURES

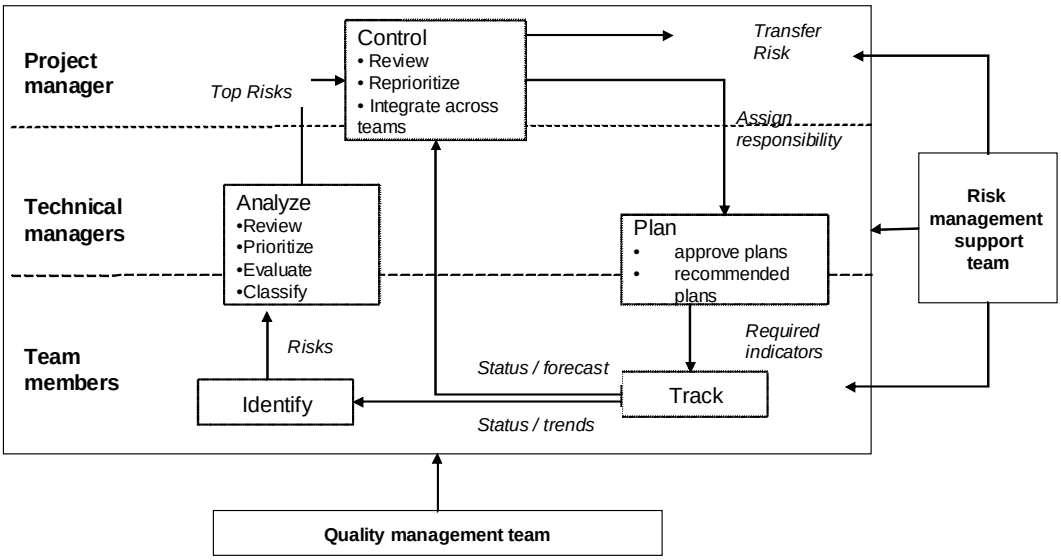

Figure 1. The different roles played by each stakeholder in the risk process.

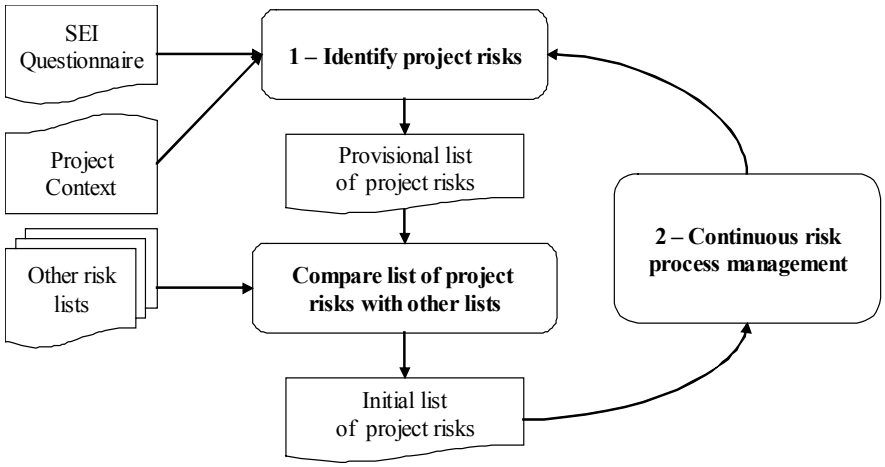

Figure 2. Risk identification framework followed in the PRISMA project.

9 TABLES

	Euromethod	Safe	SEI-CRM	IEEE	Riskit	PMI
Risk plan						●
Review define goals					●	●
Identifying risk	●	●	●	●	●	●
Risk estimation	●		●	●	●	●
Risk evaluation	●	●	●	●	●	●
Planning risk treatment	●	●	●	●	●	●
Performing risk treatment	●	●	●	●	●	●
Risk track/monitor	●	●	●	●	●	●
Communication			●			

Table 1. List of risk methods assessed in the PRISMA Project.

	Strategic	Tactical
Organizational	Sustained management support Effective organizational change management Good project scope management Adequate project team composition Comprehensive business process reengineering Adequate project sponsor role Adequate project manager role User involvement and participation Trust between partners	Dedicated staff and consultants Strong communication inwards and outwards Formalized project plan/schedule Adequate training program Preventive trouble shooting Appropriate usage of consultants Empowered decision-makers

Table 2. Organizational, strategic and tactical factors (Esteves and Pastor 2000).

Some organizational risk factors identified	Level	SEI	Esteves and Pastor (2000)
Lack of an organizational change management plan	High		Strategic
Lack of user involvement and participation	Medium		Strategic
Lack of inwards and outwards communication	Medium	X	Tactical
Inadequate training program planning and assessment	Medium		Tactical

Table 3. Some organizational risk factors identified in the PRISMA project.

NOTAS

Depósito Legal: M-20073 I.S.S.N.: 1579-4873