5

Towards Knowledge Based Risk Management Approach in Software Projects

Pasquale Ardimento[1], Nicola Boffoli[1],
Danilo Caivano[1] and Marta Cimitile[2]
[1]*University of Bari Aldo Moro, Department of Informatics*
[2]*Faculty of Economy Unitelma Sapienza, Rome*
Italy

1. Introduction

All projects involve risk; a zero risk project is not worth pursuing. Furthermore, due to software project uniqueness, uncertainty about final results will always accompany software development. While risks cannot be removed from software development, software engineers instead, should learn to manage them better (Arshad et al., 2009; Batista Webster et al., 2005; Gilliam, 2004). Risk Management and Planning requires organization experience, as it is strongly centred in both experience and knowledge acquired in former projects. The larger experience of the project manager improves his ability in identifying risks, estimating their occurrence likelihood and impact, and defining appropriate risk response plan. Thus risk knowledge cannot remain in an individual dimension, rather it must be made available for the organization that needs it to learn and enhance its performances in facing risks. If this does not occur, project managers can inadvertently repeat past mistakes simply because they do not know or do not remember the mitigation actions successfully applied in the past or they are unable to foresee the risks caused by certain project restrictions and characteristics. Risk knowledge has to be packaged and stored over time throughout project execution for future reuse.

Risk management methodologies are usually based on the use of questionnaires for risk identification and templates for investigating critical issues. Such artefacts are not often related each other and thus usually there is no documented cause-effect relation between issues, risks and mitigation actions. Furthermore today methodologies do not explicitly take in to account the need to collect experience systematically in order to reuse it in future projects.

To convey these problems, this work proposes a framework based on the Experience Factory Organization (EFO) model (Basili et al., 1994; Basili et al., 2007; Schneider & Hunnius, 2003) and then use of Quality Improvement Paradigm (QIP) (Basili, 1989).

The framework is also specialized within one of the largest firms of current Italian Software Market. For privacy reasons, and from here on, we will refer to it as "FIRM". Finally in order to quantitatively evaluate the proposal, two empirical investigations were carried out: a post-mortem analysis and a case study. Both empirical investigations were carried out in the FIRM context and involve legacy systems transformation projects. The first empirical investigation involved 7 already executed projects while the second one 5 in itinere projects. The research questions we ask are:

Does the proposed knowledge based framework lead to a more effective risk management than the one obtained without using it?
Does the proposed knowledge based framework lead to a more precise risk management than the one obtained without using it?
The rest of the paper is organized as follows: section 2 provides a brief overview of the main research activities presented in literature dealing with the same topics; section 3 presents the proposed framework, while section 4 its specialization in the FIRM context; section 5 describes empirical studies we executed, results and discussions are presented in section 6. Finally, conclusions are drawn in section 7.

2. Related works

Efficient risk management methodologies must be devised and implemented in order to avoid, minimize or transfer the risks to external entities. For this reason risk management should be a mature process integrated with all other enterprise processes (Kànel et al., 2010). Unfortunately, risk analysis is rarely fully integrated with project management in Software Engineering. While Boehm (Boehm, 1989) has lain the foundations and Charette (Charette, 1990) outlined the applications, there have been few widely developed and used formal risk methodologies tailored for software development industry. Today risk methodologies are usually based on the identification, decomposition and analysis of events that can determine negative impacts on the projects (Farias et al., 2003; Chatterjee & Ramesh, 1999; Gemmer, 1997; Costa et al., 2007). Different approaches can be adopted to deal with the key risk factors: in (Arshad et al., 2009; Hefner, 1994; Donaldson & Siegel, 2007) some risk management activities and strategies are described. In (Hefner, 1994) authors propose a methodology based on the use of capabilities and maturity models, combined with risk and value creation factors analysis to reduce risk levels. In (Donaldson & Siegel, 2007), authors propose a five step process for incorporating risk assessment and risk derived resource allocation recommendations into project plan development. Furthermore, in (Kontio, 2001; Hefner, 1994) the Riskit approach is presented. It is a risk management process that provides accurate and timely information on the risks in a project and, at the same time, defines and implements cost efficient action to manage them.
Other assessment methods for risk and hazard analysis (Petroski, 1994; Croll et al., 1997; Stratton et al., 1998) rely on people making judgments based on their experience. For safety systems a detailed knowledge of what can go wrong is an essential prerequisite to any meaningful predictions regarding the cause and effects of systems failures. In (Petroski, 1994), Petroski takes this argument further by stating that teaching history of engineering failures should be a core requirement in any engineering syllabus and take the same importance as the teaching of modern technology. Without an understanding of history or direct experience for a given application then more is unknown and hence risks are higher (Croll et al., 1997). For this reason there is a big interest towards the techniques and tools for storing and share risk knowledge. Nevertheless, the major part of today known risk management methodologies lack in doing this. They do not use any mechanism, except for human memory, to address these needs. In (Dhlamini et al., 2009) SEI SRM methodologies risk management framework for software risk management is presented. This approach is based on the adoption of three groups of practices supporting the experience sharing and communication in enterprise.

In this sense the proposed framework can be considered a complementary infrastructure for collecting and reusing risk related knowledge. Thus it can be used jointly with all the existing methodologies that it contributes to enhance.

3. Proposed framework

The proposed framework is made up of two main components: a conceptual architecture and a risk knowledge package structure for collecting and sharing risk knowledge.

3.1 Conceptual architecture

Conceptual architecture (Figure 1) is based on two well-known approaches: EFO (Schneider, 2003) and the QIP (Basili, 1989; Kànel et al., 2010).

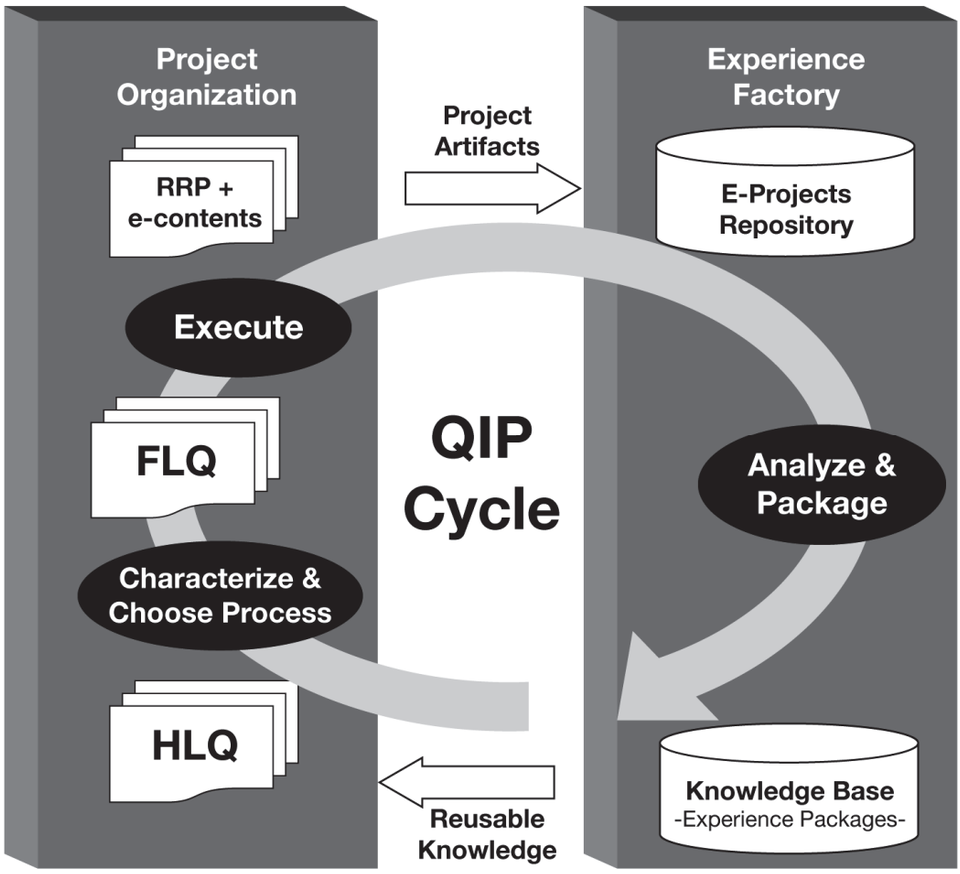

Fig. 1. Conceptual Architecture

EFO is an organizational approach for constructing, representing and organizing enterprise knowledge by allowing stakeholders to convert tacit into explicit knowledge. It distinguishes project responsibilities from those related to collection, analysis, packaging, and experience transfer activities. In doing so, it identifies two different organizational units: Project Organization (PO) and Experience Factory (EF). The first uses experience packages for developing new software solutions and the second provides specific knowledge ready to

be applied. To support these two infrastructures the QIP is used. It is based on the idea that process improvement can be accomplished only if the organisation is able to learn from previous experiences. During project execution measures are collected, and data are analysed and packaged for future use. In this sense QIP can be seen as organized in different cyclic phases (Characterize, Choose Process, Execute, Analyze and Package), that used in the organizations, perform and optimize the process of knowledge collection, packaging and transferring.

- CHARACTERIZE: it deals with the characterization of the project, the description of goals, project strategy to adopt and project planning. Such information are carried out by using focused assessment questionnaires which could have different abstraction levels (i.e. HLQ=High Level Questionnaire, FLQ=Functional Level Questionnaire). The information collected is interpreted by using the Knowledge-Base that suggests the appropriate actions to undertake in order to manage project risks.
- CHOOSE PROCESS: on the basis of the characterization of the project and of the goals that have been set, choose the appropriate processes, using the knowledge packages if present, for improvement, and supporting methods and tools, making sure that they are consistent with the goals that have been set.
- EXECUTE: it deals with the project plan execution and includes all the activities to perform for project execution. In this activities project and risk management knowledge is produces throughout project artefacts produced (e-contents) i.e. project documents, code, diagrams etc., identified risks together with the adopted mitigation actions (RRP - Risk Response Plan). They are stored in the E-Project Repository.
- ANALYZE: this phase continuously collects, analyses and generalises the information related to the executed/closed projects. After the closure of a project, such phase implies the comparison between planned and actual results, the analysis and generalization of strengths and weaknesses, risks occurred, response plans used and their effectiveness.
- PACKAGE: this phase packages experiences in the form of new, or updated and refined, models and other forms of structured knowledge gained from this and prior projects, and stores it in an experience base in order to make it available for future projects.

The proposed architecture supports the synergic integration between PO and EF. Such integration makes knowledge acquisition and reuse process incremental according to the QIP cycle that determines the improvement of the entire organization.

3.2 Structure of a knowledge package on the risk

The EFO model results to be independent from the way knowledge is represented. Nevertheless, its specialization in an operative context requires it to be tailored by using a specific knowledge representation approach.

Knowledge can be collected from several and different sources: document templates, spreadsheets for data collection and analysis, project documents, etc. In this work, an innovative approach for knowledge packaging has been defined. It is based on the use of decision tables (Ho et al., 2005; Vanthienen et al., 1998; Maes & Van Dijk, 1998).

In particular, a set of decision tables have been used to formalize knowledge first and then make it available for consultation. Knowledge means: project attributes exploitation of relations among the attributes, risks identified during project execution and consequent list of mitigation actions. According to the decision tables structure, an example of how they

have been used for representing knowledge on risk is provided (Figure 2). In the CONDITION quadrant there are project attributes (for example cost, time, available personnel, communication etc.); in CONDITIONAL STATES quadrant there are the possible values of project characteristics riskiness (based on scales different by type, at least ordinal, and depending on the attribute value which they relate to); in the ACTION QUADRANT there are risk drivers which must be taken into account (for example schedule, scarceness of personnel, etc.) together with the possible mitigation actions to carry out (for example increase the number of human resources allocated on a project, define a new date for project conclusion, etc). Finally in the RULES quadrant there are relationships between project characteristics, risk drivers and corresponding mitigation action to carrying out.

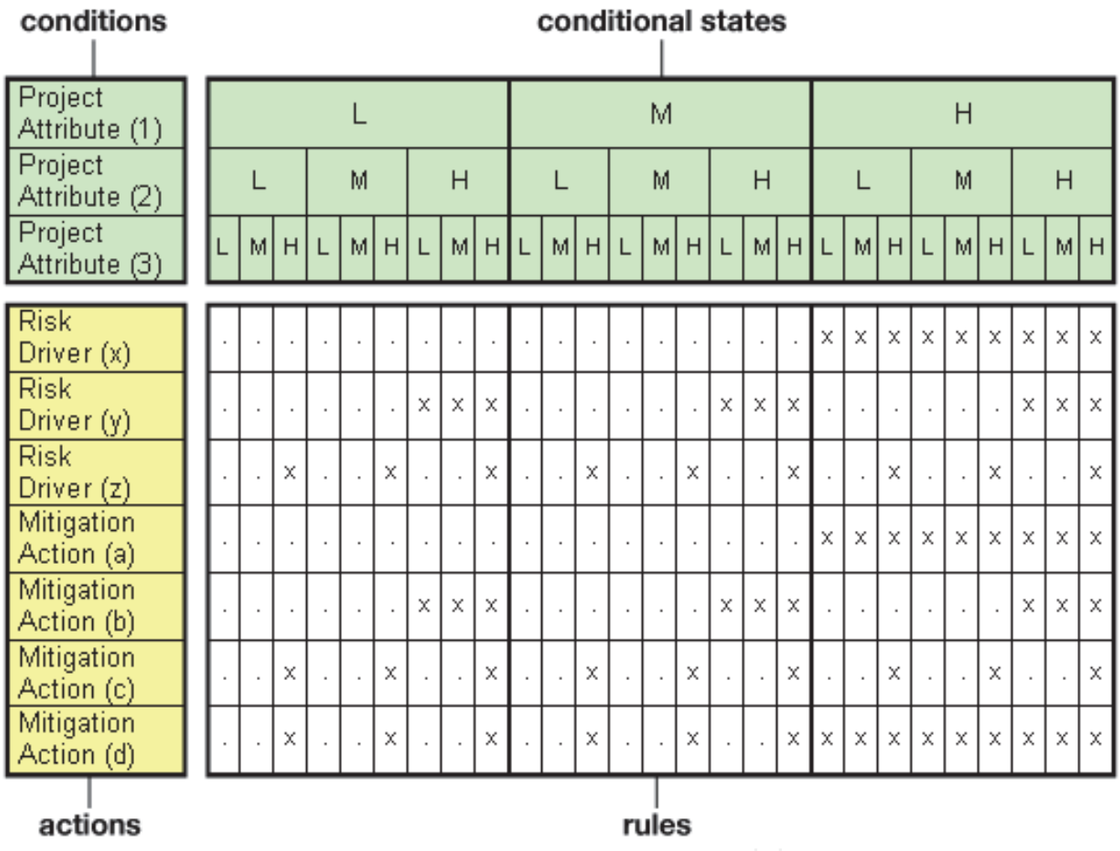

Fig. 2. An example of decision table oriented to risk management

This structure allows formalizing manager experience in risks management and, at the same time, to verify the effectiveness of the mitigation actions (Risk Response Plan). It also allows extending and updating previously acquired knowledge by adding, removing or modifying project attribute, risk driver and mitigation actions. For example, if a mitigation action results to be ineffective it can be deleted from knowledge package; project characterization, in ANALYZE and PACKAGE phases, can be enriched by adding new project attribute (i.e. context parameters).

4. Framework specialization

In order to obtain the information about FIRM context for formalizing the questionnaires and consequently the structure of the decision-tables, we carried out interviews with 50 FIRM project managers (according to the risk questionnaire in (Costa et al., 2007)). They deal with projects executed in a period of seven years. Collected data were analyzed to identify the suitable questions for risk investigation, the related risk drivers and mitigation actions. All this information was formalized as decision tables and was used to populate risk knowledge base. The steps followed were:

- Collected data by interviews were analyzed in order to extract risks from the projects occurred during their execution;
- Common risks were identified and their abstraction led us to define Risk Drivers (RD);
- Each identified risk was related to the effective mitigation actions (MA) executed;
- The most suitable questions to detect risks were identified and then related to risks;
- Questions, risks and mitigation actions were classified in relevant functional areas (Communications, Procurement, Cost, Quality, Resource, Schedule, and Scope).

The products of these activities were:

- two assessment questionnaires used to identify potential risk drivers;
- a knowledge base made of a set of decision tables used for formalizing the relationships between functional areas, risk drivers and mitigation actions

4.1 Assessment questionnaires

To identify project risks, usually the risk management process implies the use of assessment questionnaires during Risk Evaluation activity. Each questionnaire is made up of questions that support the project manager in discovering potential risks.

Typically, risk managers are supported through two different kinds of assessment questionnaires, their aim is to characterize the project by analyzing the different project management functional areas in order to assess, point out and further manage, the risks affecting a project.

In the FIRM context, two different types of questionnaires were used (example in figure 3):

High-Level Questionnaire (HLQ): questionnaire that assesses the general aspects of the projects, its aim is to generally characterize a project.

Functional-Level Questionnaire (FLQ): more specific questionnaire that points out specific issues related to the project (i.e. potential risks to mitigate), there is one specialized section for each project management functional area.

The questions of the questionnaire are answered by using a Low (L), Medium (M), High (H) scale.

The project manager starts with the HLQ for highlighting the general aspects of his project and then he uses one or more of the FLQ sections to discover the critical risk drivers and the mitigation actions related to a particular project management function (i.e. FLQs support the RRP definition).

A generalization of the relationships between HLQ, Project Management Functional Area assessed within FLQ and RD is shown in Figure 5.

It is important to underline that the use of questionnaires for knowledge execution is much diffused in industrial context, but typically, these relations between the different questionnaires and between questionnaire results and the consequent mitigation action

choice are tacit knowledge of the risk manager. Thus even when risks investigation is supported by assessment questionnaires it is usually quite subjective.
This implies the need of a risk knowledge package for collecting individual knowledge/experience previously acquired by managers during the execution of a project. The following section presents the knowledge base (i.e. a set of decision table) structured in the FIRM context.

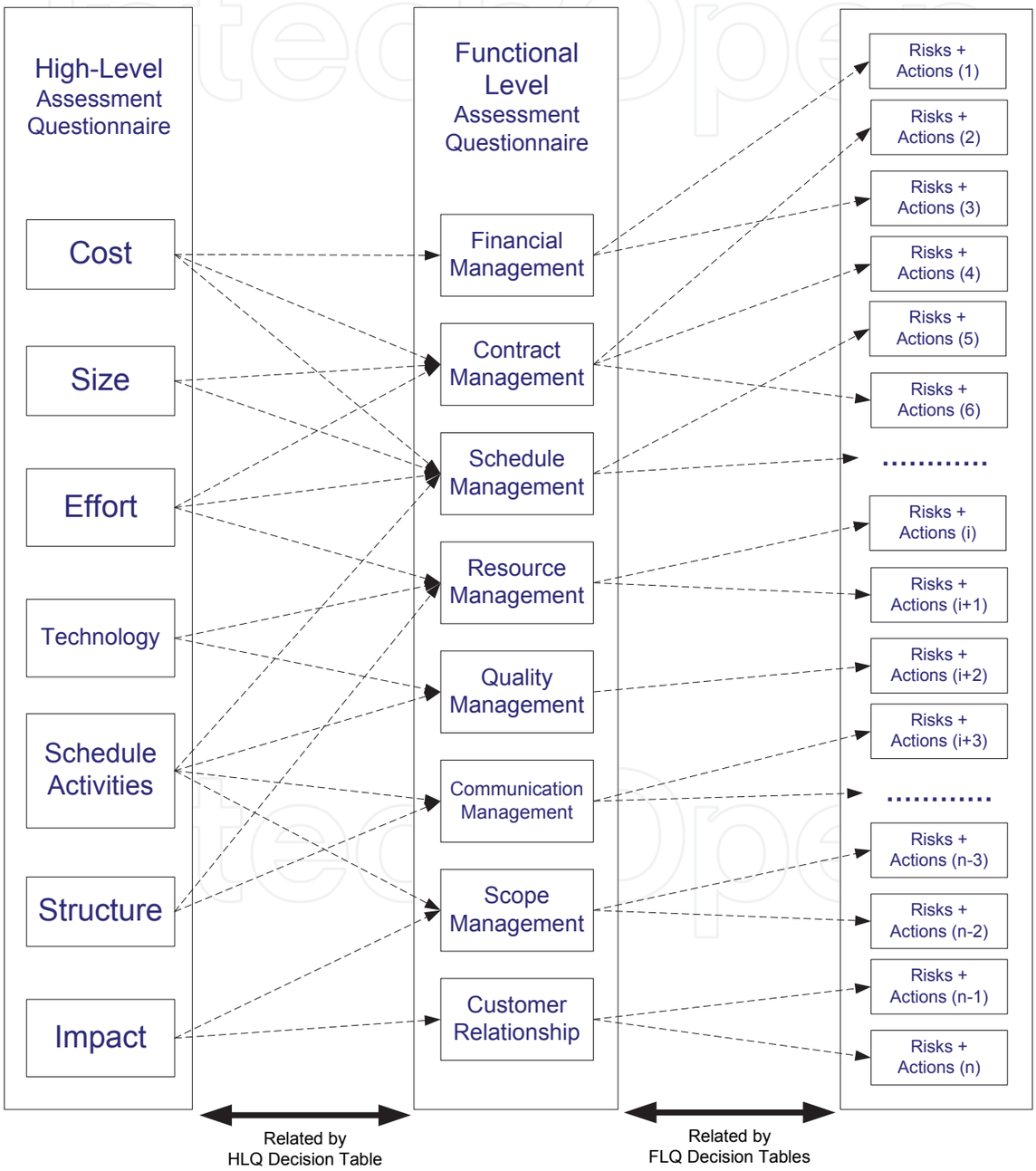

Fig. 3. Relationship schema HLQ-FLQ-Risks

4.2 Knowledge base

A set of decision tables have been used to formalize the relations between HLQ and FLQ; and to guide the project manager during the risk investigation activities. This set can be considered as an experience base. In particular, the following decision tables were introduced:

- 1 decision table for the HLQ: it relates to the general aspects of the project to more specific issues such as the functional areas of the project management that need further investigations (figure 4).
- 1 decision table for each functional area of FLQ: it relates to the specific issue of the functional area to the critical risk driver and consequent mitigation actions (figure 5).

4.2.1 Decision table supporting HLQ

In the CONDITION quadrant there are project attributes referring to general aspects of the project (for example cost, size, effort, technology, etc.); in the CONDITIONAL STATE quadrant there are possible values of project attributes (typically a Low-Medium-High scale); in the ACTION QUADRANT there are the functional areas of project management for further investigations. Finally, in the RULE quadrant there are the relationships between project attributes and the critical functional areas that need more specific investigation. An example is shown in figure 4.

1. Cost	M																H											
2. Size	H																-											
3. Effort	L or M				H												L or M											
4. Technology	H				L or M						H						L											
5. Schedule	H				L or M					H	L or M			H			L or M										H	
6. Structure	L		M or H		L or M			H			-		-				-			L			M			H		L	
7. Impact	L	M or H	L	M or H	L	M	H	L	M	H	L	M or H	L	M	H	L	M or H	L	M	H	L	M	H	L	M	H	L	M	H	L	M or H
1. ^Financial	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	x	x
2. ^Contract	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3. ^Schedule	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4. ^Resource	.	.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	.	.	.	x	x	x	x	x	x	.	.
5. ^Quality	x	x	x	x	.	.	.	.	.	.	x	x	x	x	x	x	x	.	.	.	.	.	.	.	.	.	x	x
6. ^Communication	x	x	x	x	.	.	.	x	x	x	x	x	x	x	x	x	x	.	.	.	.	.	.	x	x	x	x	x
7. ^Scope	x	x	x	x	.	.	x	.	.	x	x	x	.	.	x	x	x	.	.	x	.	.	x	.	.	x	x	x
8. ^Customer	.	x	.	x	.	x	x	.	x	x	.	x	.	x	x	.	x	.	x	x	.	x	x	.	x	x	.	x
	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283

Fig. 4. An example of decision table supporting HLQ

4.2.2 Decision tables supporting the FLQ

The CONDITION quadrant contains specific issues related to the functional area; the CONDITIONAL STATE quadrant contains the possible value of each specific issue (typically a Low-Medium-High scale); in the ACTION QUADRANT there are risk drivers that must be faced (for example schedule, scarceness of personnel, etc.) together with the possible mitigation actions to carry out (for example increasing the number of human resources allocated on a project, defining a new date for project conclusion, etc). Finally the RULE quadrant identifies the relationship between specific issues, risk drivers and corresponding mitigation actions to carry out. An example is shown in figure 5.

1. Type of project organization	L									M									H									
2. Relationship of the organizational units in the project effort	L			M			H			L			M			H			L			M			H				
3. Preparation and commitment to project status reporting	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
1. RD: Project plan requires matrix combination of personnel and production functions	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	.	.	.	.	.	.	.	.	.	.	.	.
2. MA: Require periodical meetings in the communication plan	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	.	.	.	.	.	.	.	.	.	.	.	.
3. RD: Project organization follows a matrix	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	x	x	x
4. MA: Require periodical meetings in the communication plan	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	x	x	x
5. RD: No management activity assigned to the project	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	x	x	x
6. MA: Periodical meetings to be held with the head of personnel	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	x	x	x	x	x	x	x	x	x	x	x	x
7. RD: Cooperation among organization units generates confliction	.	.	.	x	x	x	.	.	.	.	.	.	x	x	x	.	.	.	.	.	.	x	x	x	.	.	.	.	.	.
8. MA: Identify a person for each organization unit, together with tasks for each role	.	.	.	x	x	x	.	.	.	.	.	.	x	x	x	.	.	.	.	.	.	x	x	x	.	.	.	.	.	.
9. MA: Meetings in the communication plan with managers of each organization unit	.	.	.	x	x	x	x	x	x	.	.	.	x	x	x	x	x	x	.	.	.	x	x	x	x	x	x	x	x	x
10. RD: Relation among organization units generates confliction	.	.	.	.	.	.	x	x	x	.	.	.	.	.	x	x	x	.	.	.	.	.	.	x	x	x	.	.	.	.
11. MA: Also involve the higher levels of the client organizations	.	.	.	.	.	.	x	x	x	.	.	.	.	.	x	x	x	.	.	.	.	.	.	x	x	x	.	.	.	.
12. RD: Project team planned a status report, but no agreement about format/frequency	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.
13. MA: Define a standard template for the status report and identify its frequency	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.
14. RD: Project team has not planned to produce a status report	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x
15. MA: Periodical meetings with client management for illustrating project status	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x	.	.	x
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27			

Fig. 5. An example of decision table supporting FLQ

4.3 Scenario of consulting activity

The project manager answers to HLQ, each question included in HLQ corresponds to a condition (project attribute) of the related decision table; then the table interprets these responses and the actual actions are extracted. These actions are related to the functional areas of project management that need further investigation, therefore the actions guide the project manager in answering corresponding sections in the FLQ. Each section in FLQ corresponds to a specific decision table and then each selected question corresponds to a condition (specific issue) of the table which interprets these responses and then extracts the action. These actions are related to risk drivers and correspondent mitigation actions to carrying out. Therefore project managers might use issues, risk drivers and mitigation actions extracted in order to build the final Risk Response Plan (Figure 6).

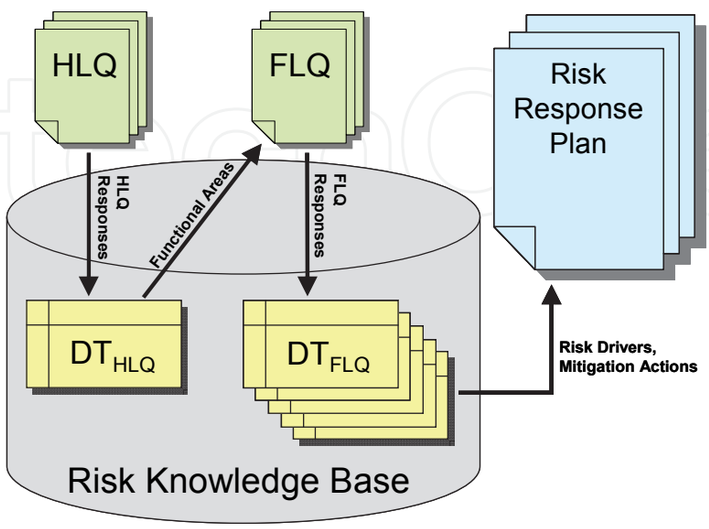

Fig. 6. Scheme of consulting activity

For example, according to Figure 4, one of the tuple corresponding to HLQ answers is (Cost, Size, Effort, Technology, Schedule, Structure, and Impact) = (M, H, H, L, L H, and L) for this tuple "Communication" is one of the critical areas to investigate. In figure 5, Communication area is investigated and one of the tuple obtained by the related FLQ is (Type of project Organization, Relationship of the organizational units in the project effort, Preparation and commitment to project status reporting) = (M, L, M). For this tuple, two selected RD corresponding to row 1 and raw 12 of decision table in Figure 5 are selected and two MA corresponding to row 2 and 13 are suggested.

5. Empirical investigation

The proposed framework has been investigated through two different types of empirical investigations: post-mortem analysis and case study.

Post-mortem analysis can be defined as "a series of steps aimed at examining the lessons to be learnt from products, processes and resources to benefit on-going and future projects. Post-mortems enable individual learning to be converted into team and organizational learning" (Myllyaho et al., 2004).

Case studies (Yin, 2003; Kitchenham et al., 1995), instead, are investigations on real projects being carried out in an industrial setting. Consequently, all variables are defined a priori, but the level of control is low. These are strongly influenced by the context of the enterprise providing the experimental environment. Also, the independent variables of the study may change due to management decisions or as a consequence to a natural evolution of the process variables considered during project execution. Generally, a case study is carried out to investigate a phenomenon within a specific range of time. A case study can be used as a means to evaluate the efficiency of a possible innovation or as a comparative study which evaluates and compares results deriving from the application of an innovative method, technique or tool and the one already in use within the enterprise.

Both post-mortem analysis and case study were executed on industrial project data of a large software firm. The goal of this firm is to embed the risk assessment/treatment in its primary processes in order to support its project execution by the experience acquired in former projects. Therefore FIRM, jointly with the Department of Informatics of Bari, has introduced the approach for highlighting and managing the risks occurred.

To execute post mortem analysis, also called simulation, 54 projects of FIRM have been analyzed, all executed in a period of seven years, and seven of them, considered homogeneous in terms of duration, project size and development team experience, were selected.

Furthermore to execute the case study, 5 projects have been analyzed in-itinere in order to directly evaluate the appropriateness of the proposed framework.

Both investigations aim at evaluating the proposed approach with respect to the same factors, in the same context and with the same viewpoint. For these reasons the experiment definition and the metric model adopted, explained in the following, are the same.

5.1 Experiment definition

The aims of the empirical investigation are to verify whether risk management resulting from the application of Proposed Approach (PA) is more efficient and precise than risk management carried out using traditional Management Support (MS), i.e. the traditional risk management.

Effectiveness means the ability to undertake mitigation actions that, for each expected risk, avoid that a risk degenerates in one or more problems. While Precision is the ability to foresee all the occurred risks.
Research goals are thus formalized as follow:

RG1. *Analyze* the proposed approach *for the purpose of* comparing it to risk management obtained by only using management support with respect to Effectiveness *from viewpoint of* FIRM risk manager *in the context of* industrial FIRM projects	***RG2***. *Analyze* the proposed approach *for the purpose of* comparing it to risk management obtained by only using management support with respect to Precision *from viewpoint of* FIRM risk manager *in the context of* industrial FIRM projects

The consequent research hypotheses to test were:

- H_0Effectiveness: there is no statistically significant difference in effectiveness between PA and MS.
- H_1Effectiveness: there is statistically significant difference in effectiveness between PA and MS.
- H_0Precision: there is no statistically significant difference in precision between PA and MS.
- H_1Precision: there is statistically significant difference in precision between PA and MS.

Independent variables represent the two treatments: risk management using proposed approach (PA) and risk management using only management support (MS).
Dependent variables were quality characteristics of research goals, i.e. effectiveness and precision. Both these variables were operatively quantified by using the metrics presented in the next paragraph.

5.2 Metric model

The following metrics were used to quantitatively asses the research goals:

$$Effectiveness = \left(1 - \frac{NOP}{NMR}\right) * 100$$

$$Effectiveness\,Gain = \left(\frac{Effectiveness\,of\,PA}{Effectiveness\,of\,MS} - 1\right) * 100$$

$$Precision = \left(\frac{NER}{NER + NUR}\right) * 100$$

$$Precision\,Gain = \left(\frac{Precision\,of\,PA}{Precision\,of\,MS} - 1\right) * 100$$

Where:

- Number of Expected Risk (NER): number of Expected Risks during project execution taken into account by project manager.
- Number of Unexpected Risk (NUR): number of occurred risks that are not foreseen (Unexpected Risk).
- Number of Managed Risk (NMR): number of expected risks managed by using a specific strategy.

- Number of Occurred Problems (NOP): number of problems (OP) raised during project execution because of degeneration of an expected risk badly managed. Each OP identifies a single occurred problem or a set of them. For these reasons NMR >= NOP

Figure 7 shows relationships among metrics in terms of sets.

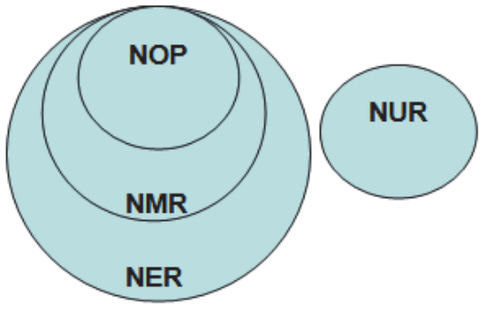

Fig. 7. Relationships between metrics

Note that Effectiveness can be equal to zero or, at maximum, equal to 100%. When Effectiveness is:

- Tends to 100% all the Expected Risks are well managed, in particular when NOP tends to zero;
- Tends to 0% when no one of the Expected Risk is well managed. In particular when NOP tends to NMR.

Therefore Effectiveness means the capability to manage the risks and to put to use the related mitigation actions in the way to avoid they became problems during the project execution. For this reason Effectiveness is as grater as smaller is the NER that became problems.

Precision can tend to zero or, at maximum tend to 100%. When Precision:

- Tends to 100%, when all the possible risks were detected, in particular when UR tends to 0.
- Tends to 0% at the NUR increasing, in particular it means that number of UR is much greater than NER.

In fact Precision means the capability to foresee all the risks that can occur during project execution NUR decreases.

At the beginning of each project and iteratively during project execution, a manager points out a set of Expected Risks. Part of this set, composed by the most critical and relevant risks for the project, will be managed, while the remaining ones, will not. In general terms, a risk is managed when a risk response plan is developed for it.

Action strategy defined by the manager for each MR in some cases is successful and in other cases transforms a risk into an OP. The last case is indicative of ineffectiveness of the strategy action adopted in the project execution. Finally it is also possible that some problems (UP), raised during project execution, are related to UR.

6. Data analysis

Proposed approach was validated using “Post Mortem Analysis” and “Case Study”. Both in Post Mortem Analysis and in Case Study according to the experimental design, statistical analysis were carried out. First of all descriptive statistics were used to interpret data

graphically. Data collected during experimentation have been synthesized through descriptive statistics. Finally, data have been analysed through hypothesis testing, where initial hypothesis were statistically validated with respect to a significance level. The dependent variables were tested in order to investigate the significance of the differences observed in the values collected.
In next paragraphs the results of data analysis are given. The first paragraph (6.1) refers to post mortem analysis and the second one (6.2) to the case study

6.1 Post mortem analysis

This investigation aims at evaluating the PA effectiveness and precision by observing the model behaviour used on legacy data related to projects already executed with the traditional approach.
Data set includes 14 observations, 2 for each project.

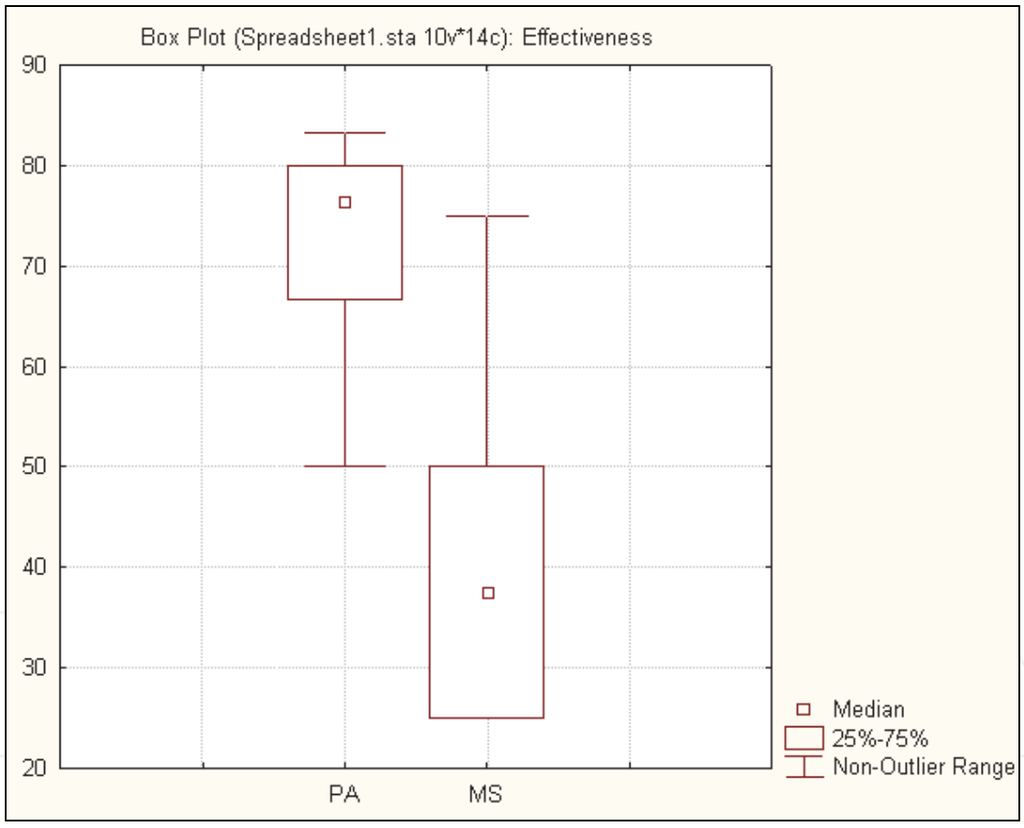

Fig. 8. Box plot for effectiveness (median)

Figure 8 shows the box plot related to the effectiveness of MS and PA. As it can be seen there is a greater effectiveness of PA than MS in terms of median value, 76.39% against 37.50%, and of lower and upper quartiles values , [66.67%, 80.00%] for PA and [25.00%, 50.00%] for MS.
The result of the descriptive analysis is statistically significant according to the Wilcoxon test. Wilcoxon test (Wilcoxon, 1945) is the nonparametric alternative to t-test for dependent samples. Since normality conditions were not always met, non parametric test was chosen. We used Shapiro-Wilk W test to verify if normality conditions were always satisfied or not.

Experimental Group	p-level	Results
Effectiveness	0.0210	reject $H_{0Effectiveness}$ and accept $H_{1Effectiveness}$

Table 1. P-level value of the Wilcoxon test for Effectiveness value

The test points out a significant difference in the Effectiveness between the two approaches. Therefore the null hypothesis can be rejected and we can conclude that the proposed approach is more efficient than traditional risk management.
Figure 9 shows the median values of precision of PA and MS. As it can be seen there is a greater precision of PA than MS in terms median value, 71.43% against 50.00%, and of lower and upper quartiles values, [50.00%, 75.00%] for PA and [33.33%, 66.67%] for MS.

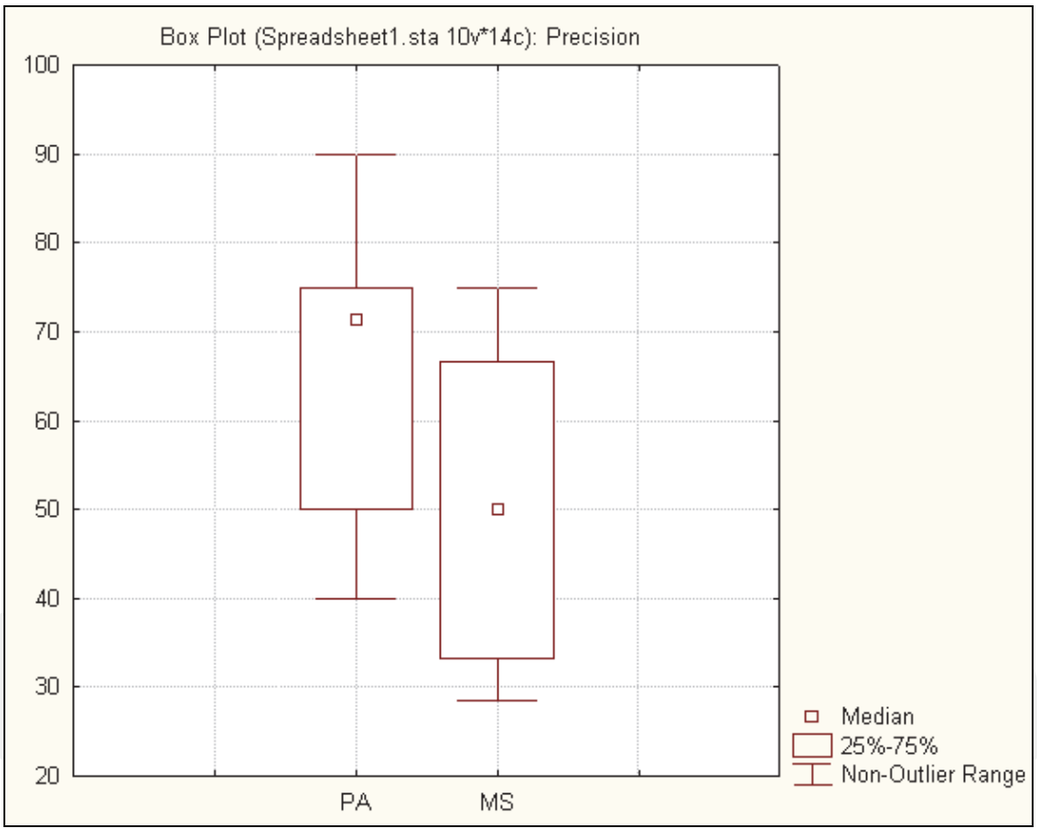

Fig. 9. Box plot for precision (median)

Also in this case Shapiro-Wilk W test was used to test normality. Since observed values were not normally distributed, also in this case, the Wilcoxon test was used.
Table 2 reports the values of the p-level obtained by using Wilcoxon test, applied to Precision of the two approaches. The test points out a significant difference between the two approaches. Therefore the null hypothesis can be rejected and we can conclude that the proposed approach is more precise in risk management.

Experimental Group	p-level	Results
Precision	0.0253	reject $H_{0Precision}$ and accept $H_{1Precision}$

Table 2. P-level value of the Wilcoxon test for Precision value

6.2 Case study data analysis

This kind of investigation evaluates PA effectiveness and precision, compared with MS, measuring it "on the field" during the execution of some processes. For this purpose, 5 projects that conducted with the both approaches were selected. As for the post mortem analysis, also in this case, the collected values appeared as not be normally distributed and thus the Wilcoxon non parametric test was used for the hypotheses testing the α-value was fixed at 5%.

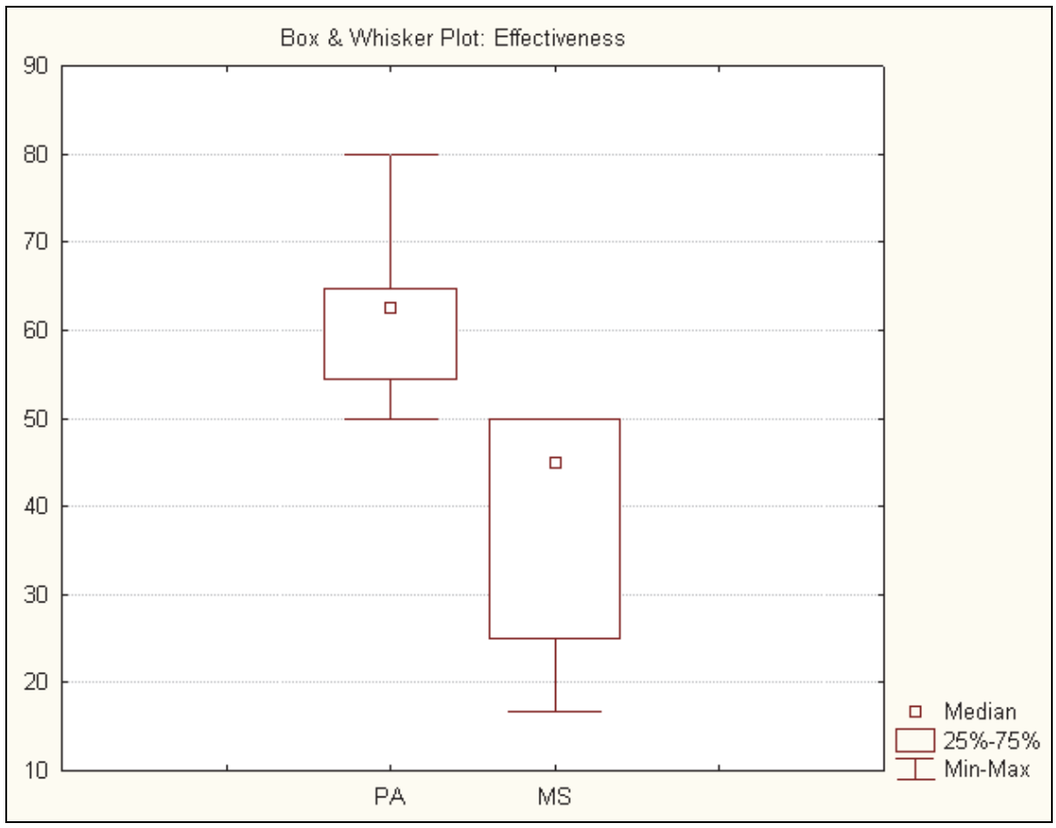

Fig. 10. Box plot for effectiveness (median)

Figure 10 shows the box plot related to the effectiveness of MS and PA. As it can be seen there is a greater effectiveness of PA than MS in terms of median value, 62.50% against 45.00%, and of lower and upper quartiles values, [54.54%, 64.70%] for PA and [25.00%, 50.00%] for MS. Regarding the distribution, data seem to confirm what was seen in post mortem analysis.

Table 3 reports the values of the p-level resulted from the Wilcoxon test applied to the Effectiveness of MS and PA.

Experimental Group	p-level	Results
Effectiveness	0.0009	reject $H_{0Effectiveness}$ and accept $H_{1Effectiveness}$

Table 3. P-level value of the Wilcoxon test for Effectiveness value.

The test points out a significant difference in the Effectiveness between the two approaches. Therefore the null hypothesis can be rejected and we can conclude that the proposed approach is more efficient than the manager approach. The Case Study allows to reject the null hypothesis with the error probability lower than in the case of the post-mortem analysis.
Figure 11 shows the median values of precision of PA and MS. As it can be seen there is a greater precision of PA than MS in terms median value, 71.57% against 50.00%, and of lower and upper quartiles values, [50.00%, 80.00%] for PA and [50.00%, 60.00%] for MS.

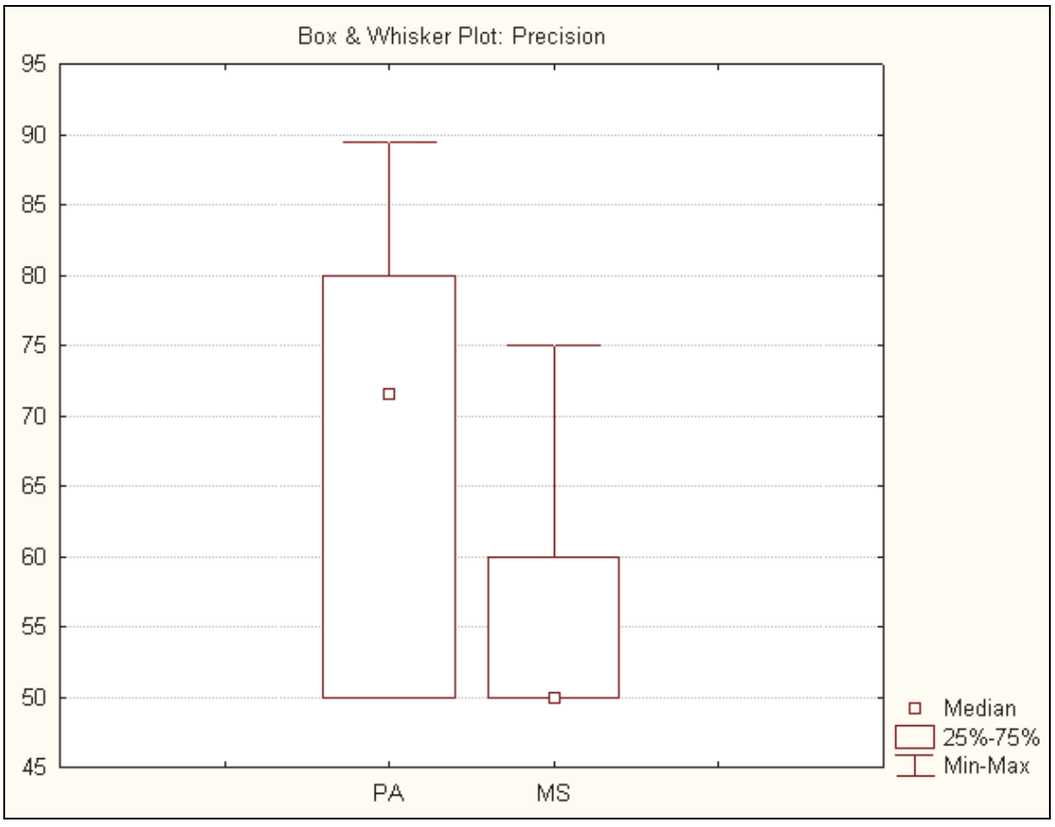

Fig. 11. Box plot for precision (median)

Table 4 reports the values of the p-level obtained by using the Wilcoxon test, applied to Precision of the two approaches. There is, also in this case, a statistically significant difference in the Precision between the two approaches, i.e. the null hypothesis can be rejected concluding that the proposed approach is more precise than the manager approach. Also in this case, the test points out a significant difference between the two approaches. Therefore the null hypothesis can be rejected and we can conclude that the proposed approach is more precise in risk management.

Experimental Group	p-level	Results
Precision	0.005	reject $H_{0Precision}$ and accept $H_{1Precision}$

Table 4. P-level value of the Wilcoxon test for Precision value

6.3 Lessons learnt

An additional experimentation data analysis allowed us to make some general qualitative considerations completing the comparison between the PA and the MS.

To make these analyses we consider the issues areas that were listed in the FLQ (Figure 3):

- Financial Management
- Contract Management
- Schedule Management
- Resource Management
- Quality Management
- Communication Management
- Scope Management
- Customer Relationship

We decided to consider the FLQ issues areas because we valuate this detail level the better one on the base of the number of collected data.

According to the Post Mortem data, the critical areas (the areas that were characterized by the higher number of problems) were: Resource Management, Quality Management, and Scope Management.

Resource Management consists of human resources and infrastructure management. Infrastructure management requires the identification and acquisition of all necessary equipment capable to carry out the project.

Quality Management consists of planning, constructing and evaluating product and service quality. This function requires, in particular, planning and conducting of quality assurance reviews, or reviews aimed at evaluating the quality of the process.

Finally, Scope Management consists of Defining the product or service expected by the consumer (product scope) and the corresponding work necessary to achieve it (project scope); also monitoring changes during the project execution.

For the critical areas we observed that MS finds a lower NER than the PA. Moreover, while in MS only a few part of NER are managed, in PA all the NER are managed. Moreover, in the PA the NUR is lower than in MS, it could be a consequence of the better capacity of PA to find risks and to manage them. These observations could consequently motivate the quantitative Precision Post Mortem results.

According to the Post Mortem data, we found in the Case Study the same critical issues areas but in this case there was a decreasing of the PA criticality. This reduction could confirm that the approach based on the EF tends to improve the capacity to manage the risk in the critical areas towards the past experiences that were acquired in these areas. In fact the higher number of experiences, of data and of practices is usually related to the most critical areas. According to this consideration, we observed that the reduction of occurred problem in PA is consequence of the increase of the number of mitigation action efficacy.

7. Conclusions

This paper proposes a Knowledge based Risk Management Framework able to collect, formalize and reuse the knowledge acquired during past projects execution. As instrument for supporting such methodology, an appropriate set of assessment questionnaires and decision-tables have been proposed. The innovative use of decision tables allowed to capture risk knowledge during the entire project lifecycle and to improve the knowledge collected in the Knowledge Base.

Thanks to knowledge expressed through decision tables, the proposed approach allows to combine the results of each document for evaluating the effects and the possible mitigation actions. In other words it allows express:

The relations between generic and specific issues;

The relations between issues, risks and actions to undertake to mitigate the risks as they occur.

To evaluate the proposed approach the framework has been transferred and investigated in an industrial context through two different types of empirical investigations: post-mortem analysis and case study.

Research goals aimed at assessing whether the proposed approach was more effective and precise for supporting risk management in software processes compared to traditional risk management approaches for Management Support.

Data analysis pointed out a statistically significant difference between the proposed approach and the traditional one in software process risk management with respect to effectiveness and precision. Such empirical results confirm that better structured risk knowledge, customizable according to the context, helps a manager to achieve more accurate risk management. Moreover we observed that the proposed approach allowed, especially in the critical areas such as Resource Management, Quality Management, Scope Management, to obtain better results. Obviously, in order to generalize the validity of the proposed approach further studies extended to other contexts are needed. For this reason, the authors intend replicating the empirical investigations.

8. References

Arshad, N.H., Mohamed, A., & Mansor, R. (2009). Organizational structural strategies in risk management implementation: best practices and benefits, WSEAS Transactions on Information Science and Applications, Vol. 6, No. 6, June 2009

Basili, V.R. (1989). Software Development: A Paradigm for the Future, Proceedings of the Annual Computer Software and Applications Conference, Orlando, September 1989

Basili, V.R., Bomarius, F., & Feldmann. (2007). Get Your Experience Factory Ready for the Next Decade: Ten Years After Experience Factory: How to Build and Run One, Proceedings of IEEE Int. Conf. on Software Maintenance, Minneapolis, May 2007

Basili, V.R., Caldiera, G., & Rombach, H.D. (1994). The Experience Factory. Encyclopedia of Software Engineering, John Wiley & Sons, Inc., 1994

Batista Webster, K.P., de Oliveira, K.M., & Anquetil, N. (2005). A Risk Taxonomy Proposal for Software Maintenance, Proceedings of IEEE Int. Conf. on Software Maintenance, Budapest, September, pp. 2005

Boehm, B.W. (1989). Tutorial: Software Risk Management, IEEE Computer Society Press, New. York, 1989

Charette, R.N. (1990). Application Strategies for Risk Analysis, McGraw-Hill Book Company, ISBN 0-07-010888-9, 1990

Chatterjee, D., & Ramesh, V.C. (1999). Real Options for Risk Management in Information Technology Projects, Proceedings of Hawaii International Conference on System Sciences, Maui, January 1999

Costa, H.R., de O. Barros, M., & Travassos, G. H. (2007). Evaluating Software Project Portfolio Risks, Journal of Systems and Software, Vol. 80, No. 1, pp. 16-31, 2007

Croll, P.R., Chambers, C., Bowell, M., & Chung, P.W.H. (1997). Towards Safer Industrial Computer Control Systems, Proceedings of International Conference On Computer Safety, Reliability and Security, York, September, 1997

Dhlamini, J., Nhamu, I. & Kaihepa. (2009). Intelligent risk management tools for software development, Proceedings of the 2009 Annual Conference of the Southern African Computer Lecturers' Association (SACLA '09), ACM, New York

Donaldson S. E. & Siegel, S. G. (2007). Enriching Your Project Planning: Tying Risk Assessment to Resource Estimation, IT Professional, Vol. 9, No 5, pp.20-27, 2007

Farias, L., Travassos, G.H., & Rocha, A.R. (2003). Managing Organizational Risk Knowledge, Journal of Universal Computer Science, Vol. 9, No. 7, 2003

Gemmer, A. (1997). Risk Management: Moving Beyond Process, IEEE Computer, Vol. 30, No. 5, pp. 33-43 , 1997

Gilliam, P.D. (2004). Security Risks: Management and Mitigation in the Software Life Cycle, Proceedings of IEEE Int. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Modena, June 2004

Hefner, R. (1994). Experience with Applying SEI's Risk Taxonomy, Proceedings of Conference on Software Risk Management, Pittsburgh, 1994

Ho, T.B., Cheung, D., & Liu, H. (2005). Advances in Knowledge Discovery and Data Mining, LNCS Springer, Heidelberg

Kànel V. J., Cope, E. W., Deleris, L. A., Nayak, N. & Torok, R. G. (2010). Three key enablers to successful enterprise risk management. IBM Journal of Research and Development, Vol. 54, No. 3, May 2010

Kitchenham, B., Pickard, & L., Pfleeger, S.L. (1995), Case Studies for Method and Tool Evaluation, IEEE Software, Vol. 12, No 4, pp. 52-62

Kontio, J. (2001). Software Engineering Risk Management: A Method, Improvement Framework and Empirical Evaluation, R&D-Ware Technical Report, 2001

Loon, H.V. (2007). A Management Methodology to Reduce Risk and Improve Quality, IT Professional, Vol. 9, No 6, pp.30-35, 2007, ISBN 1520-9202

Maes, R.J., & Van Dijk, E.M. (1998). On the Role of Ambiguity and Incompleteness in the Design of Decision Tables and Rule-Based Systems, The Computer Journal, Vol. 31, No. 6, pp. 481-489

Myllyaho, M., Salo, O., Kääriäinen, J., Hyysalo, J., & Koskela, J. (2004) . A Review of Small and Large Post-Mortem Analysis Methods, Proceedings of International Conference on Software and Systems Engineering and Their Applications, Paris, 2004

Petroski H. (1994). Design Paradigms: Case Histories of Error and Judgment in Engineering, Cambridge University Press, ISBN 0-521-46649-0

Schneider K., & Hunnius, J.V. (2003). Effective Experience Repositories for Software Engineering, Proceedings of International Conference on Software Engineering, Portland, May 2003

Stratton, A., Holcombe, M., and Croll, P.R. (1998). Improving the Quality of Software Engineering Courses through University based Industrial Projects, Proceedings of International Workshop on the Projects in the Computing Curriculum, Sheffield, 1998

Vanthienen, J., Mues, C., Wets, G., & Delaere, K. (1998). A Tool Supported Approach to Inter-Tabular Verification, Expert Systems with Applications, Vol. 15, No. 3-4, pp. 277-285

Wilcoxon, F.(1945). Individual Comparisons by Ranking Methods, Biometrics Bulletin, Vol. 1, No 6, pp. 80-83

Yin, R.K.(2003), Case Studies Research Design and Methods, Sage Publications, ISBN 0-7619-2552-X

Risk Management Trends

Edited by Prof. Giancarlo Nota

ISBN 978-953-307-314-9
Hard cover, 266 pages
Publisher InTech
Published online 28, July, 2011
Published in print edition July, 2011

In many human activities risk is unavoidable. It pervades our life and can have a negative impact on individual, business and social levels. Luckily, risk can be assessed and we can cope with it through appropriate management methodologies. The book Risk Management Trends offers to both, researchers and practitioners, new ideas, experiences and research that can be used either to better understand risks in a rapidly changing world or to implement a risk management program in many fields. With contributions from researchers and practitioners, Risk Management Trends will empower the reader with the state of the art knowledge necessary to understand and manage risks in the fields of enterprise management, medicine, insurance and safety.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Pasquale Ardimento, Nicola Boffoli, Danilo Caivano and Marta Cimitile (2011). Towards Knowledge Based Risk Management Approach in Software Projects, Risk Management Trends, Prof. Giancarlo Nota (Ed.), ISBN: 978-953-307-314-9, InTech, Available from: http://www.intechopen.com/books/risk-management-trends/towards-knowledge-based-risk-management-approach-in-software-projects

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen