



## Risk management applied to software development projects in incubated technology-based companies: literature review, classification, and analysis

**Gestão de riscos aplicada a projetos de desenvolvimento de software em empresas de base tecnológica incubadas: revisão, classificação e análise da literatura**

Sandra Miranda Neves<sup>1</sup>  
Carlos Eduardo Sanches da Silva<sup>2</sup>

Financial support: CAPES and Fapemig.

**Abstract:** Software projects are subjected to several risk analyses, since risk related information can improve managers' decision making. This paper aimed at performing a review, classification, and analysis of the literature on risk management applied to software development projects, with an emphasis on incubated technology based companies. This theoretical-conceptual research is justified for two reasons: first, because the bulk of the research literature has not sufficiently addressed this subject; and second, because a diagnostic study carried out with incubated technology based companies emphasized the importance of this subject to them. The literature used as the grounds for this study was selected from Brazil's Coordination of Improvement for Higher Education Personnel (CAPES) database of periodicals, and classified by year of publication, place where research was conducted, type of study and approach, research aim, and research focus. We also conducted a survey of the most relevant current studies on risk management for software development projects, which revealed that studies on this issue, aimed at incubated technology based companies, are scarce. This indicates the need for empirical research to assist incubated companies in the identification of main risk factors for their business while reducing or eliminating the likelihood of failures.

**Keywords:** Risk management; Software development; Incubated technology based company.

**Resumo:** *Projetos de software estão sujeitos a uma série de riscos e identificá-los auxilia os gestores a tomar decisões de uma forma mais sistemática. O objetivo deste artigo é apresentar uma revisão, classificação e análise da literatura sobre o gerenciamento de riscos em projetos de desenvolvimento de software com ênfase em empresas de base tecnológica incubadas. O estudo, de cunho teórico-conceitual, é justificado pela existência de lacunas na literatura e por um diagnóstico realizado em empresas de base tecnológica incubadas ter indicado a importância do tema para as mesmas. As publicações selecionadas foram localizadas por meio de consultas nas bases de dados dos periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e foram classificadas de acordo com o ano de publicação, local onde as pesquisas foram realizadas, filiação, tipo de estudo, abordagem, objetivo e foco da pesquisa. Realizou-se também um levantamento dos principais resultados de pesquisas atuais sobre gerenciamento de riscos em projetos de desenvolvimento de software, cujos resultados mostram que trabalhos relativos ao tema e direcionados a empresas de base tecnológica incubadas ainda são escassos, necessitando-se de pesquisas empíricas que possam auxiliar essas empresas a identificar os seus principais fatores de riscos e a reduzir ou eliminar a probabilidade de falhas nos projetos.*

<sup>1</sup> Universidade Federal de Itajubá – UNIFEI, Campus Itabira, Rua Irmã Ivone Drumond, 200, Distrito Industrial II, CEP 35903-087, Itabira, MG, Brazil, e-mail: sandraneves@unifei.edu.br

<sup>2</sup> Universidade Federal de Itajubá – UNIFEI, Campus Prof. José Rodrigues Seabra, Avenida BPS, 1303, Pinheirinho, CEP 37500-903, Itajubá, MG, Brazil, e-mail: sanches@unifei.edu.br

**Palavras-chave:** *Gerenciamento de riscos; Desenvolvimento de software; Empresas de base tecnológica incubadas.*

## 1 Introduction

Software projects are complex undertakings in any context, and are particularly susceptible to failures (Bannerman, 2008). One of the reasons for these failures can arise from not managing the risks present in the software development project. According to Pinna & Carvalho (2008), if risks are not managed properly, the quality of the final product can be compromised; customer expectations go unmet; and staff, anxious and conflicted during the life of the project, may demonstrate reduced productivity. Conceptually, from an organizational perspective, the risk arises when organizations pursue opportunities in the face of uncertainty, and constrained by capacity and costs (Bannerman, 2008).

A number of software and project managers see the activities and processes of risk management as extra work and expense, and the risk management process is the first activity to be removed from the project scope when a project falls behind schedule (Kwak & Stoddard, 2004). These authors also state that many software development professionals perceive risk management and control as an inhibitor to creativity. The high failure rates associated with information systems projects suggest that organizations need to improve not only their ability to identify the risks associated with these projects, but also to manage them (Jiang et al., 2001).

Based on this information, this article aims to present a review, classification, and analysis of the current literature on risk management in software development projects, thereby enabling the assessment of trends and gaps in the literature on the use of risk management in micro and small incubated technology-based companies. This work is theoretical and conceptual in nature. It is a discussion arising from a literature review, which resulted in the raising of a number of relevant points (Miguel, 2007; Wacker, 2004). To develop the study we carried out a literature review of the risk management process, which sought to identify in the scientific literature works whose primary or secondary theme addressed risk management in software development projects. For this search we used the database of the Coordination for the Improvement of Higher Education Personnel (CAPES), a foundation within Brazil's Ministry of Education, selected because of its wide scope and ease of access for most Brazilian researchers (Carnevali & Miguel, 2007).

The article is structured as follows: Section 1 presented an introduction, objectives and justifications.

Section 2 illustrates the relevance of the research conducted in incubated technology-based companies and of risk management in software development projects; the data collection is outlined in Section 3, and Section 4 presents the analysis and results. Finally, Section 5 offers discussions and conclusions, as well as suggestions for further research.

## 2 Relevance of research in incubated technology-based companies

According to Kendrick (2003), all projects have risks, but high-technology projects have particular risks, such as their high variation. Although there may be similarities with project work done in the past, each project has unique aspects and objectives that substantially differ from previous work, as well as challenges to execute them faster and faster. Dahlstrand (2007) defines a technology-based company as one that depends on technology for its growth and survival, although this does not necessarily mean that the technology must be new or innovative.

According to Costa et al. (2007), risk management has gained importance in managing software projects, and the uncertainties faced in these projects should be taken into account at the time of planning and control. Lahorgue & Hanefeld (2004) highlight the importance of technology-based companies (TBCs), stating that those supported by incubators take university research technologies and place them on the market, benefiting existing businesses or consumers. Risk management as a formal structure, despite its importance, is still considered a minor tool in organizations.

In Brazil, a survey conducted in 2001 by the Department of Information Technology Policy (SEPIN) of the at the Ministry of Science and Technology (Sepin/MCT) on software engineering practices during development and maintenance, concluded that only 11.8% of the 446 participating organizations implemented risk management in their projects, and only 9.7% had risk identification documents (Brasil, 2002). It is noteworthy that, considering the total workforce of the participating organizations, 61.5% were micro and small businesses. Although information about project management, and risk management in this context, is commonly found in the literature applied to large companies (White & Fortune 2002; Bryde, 2003), little has been published on project management in small and medium enterprises (Murphy & Ledwith, 2007).

The Product Development Center (PDC) of the Technology-Based Incubator of the city of Itajubá (TBI) examined thirteen micro and small incubated

technology-based enterprises (ITBEs), and found that many projects—almost all—are conducted without the use of risk management methodologies, and that 70% of these companies consider risk analysis an improvement opportunity (Figure 1), as it could prevent, mitigate, transfer, or even accept risk, if properly managed.

After conducting a review of risks in the software development process, Bannerman (2008) concluded that there is a need for better risk management, both in research and in practice.

Unfortunately, despite these recommendations, there are relatively few tools available to help project managers to identify and categorize risk factors, in order to develop effective strategies (Wallace et al., 2004a, p. 115).

For the ITBEs evaluated, the process of risk analysis would result in a fault-prevention process, thereby enabling decision-making based on organized data. Also, an appropriate review of risks in the software development process may indicate prospects for future study, identifying gaps and furthering the conduction of research in the technology-based business incubator environment.

### 3 Risk management in software development projects

Software projects are high-risk activities, generating variable performance outcomes (Charette, 2005). According to Kerzner (2006, p. 10), the allies of project management began emerging in 1985, and risk management surfaced in 1996, when companies recognized that

[...] risk management involves more than padding an estimate or a schedule. Risk management plans are now [were then] included in the project plans [...].

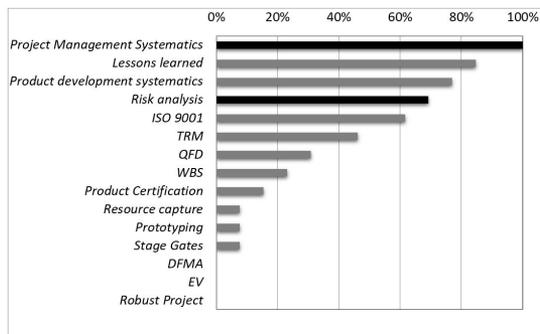


Figure 1. ITBE Diagnosis Result - 2008/2009.

A risk can be composed of two components: the probability that a loss will occur, and the importance or magnitude of this possible loss (Barki et al., 1993).

According to the Project Management Body of Knowledge, PMBoK (PMI, 2008, 194), project risk

is an uncertain event or condition which, if it occurs, has a positive or negative effect on one or more project objectives, such as scope, schedule, cost, or quality.

Risks in software projects encompass a number of factors or conditions that may pose a serious threat to the successful completion of the project (Wallace et al., 2004a); managing risk involves quantifying its importance, evaluating its probability of occurrence and its possible impact on project performance, as well as the development of strategies to control it (Huang & Han, 2008).

A study published in the Standish Group’s *Chaos Report* (The Standish Group, 2000) showed that only 28% of projects in that year were successful—delivered on time, on budget, and with required features and functions. Another 49% were challenged—late, over budget and/or lacking some required features and functions. The remaining 23% were cancelled before completion. Emam & Koru (2008) criticized this report, stating that a reasonable number of professionals and researchers questioned this research as its methodology was undisclosed, it was not submitted to peer review, and was inconsistent in defining the failures. In a similar survey conducted by the same authors in order to evaluate cancellation and success rates, a cancellation rate of 15.52% in 2005 and 11.54% in 2007 was obtained; 48% to 55% of the projects were deemed to have been successfully delivered; and 17% to 22% were considered failures. The combined rate of failure and cancellations dropped from 34% in 2005 to 26% in 2007, suggesting a trend towards improvement. Despite this, many software development projects still use more resources than planned, take too long to complete, and provide less quality and functionality than expected (Barros et al., 2004). But why do software projects fail so often?

- According to Kwak & Stoddard (2004), Project failures are the result of a multiplicity of inherent risks in software project environments.

- According to Charette (2005), the most common factors are: unrealistic goals; inaccurate estimates of needed resources; badly defined system requirements; poor reporting of the project’s status; unmanaged risks; miscommunications between customers, developers, and users; use

of immature technology; inability to cope with project complexity; sloppy developed practices; mismanagement of the project; stakeholder politics; and commercial pressures;

- Although some managers claim that they manage the risks in their projects, there is evidence that they do not do so systematically. Some may assess technical risks at the expense of market and financial risks, which are just as vital to software development success (Dey et al., 2007);
- According to Barros et al. (2004), most of the techniques applied to software development projects require clear and defined objectives; time and resources allocated before the start of the project; and well-defined quality metrics, among other needs, which are usually not available to large projects;
- Changes in project requirements and scope are the main reasons for project cancellation (Emam & Koru, 2008).

Raz et al. (2002), Jiang et al. (2001), Wallace et al. (2004a) all contend that risks can be successfully managed. According to Saarinen (1996), the success factors in implementing projects should cover four areas: success of development process; success of the use process; quality of product; and impact on the organization. Dey et al. (2007) posit that a successful project depends on criteria such as functionality, quality, and timeliness.

Identifying the risks associated with the implementation of Information Technology (IT) projects can become a major challenge for managers, since there are various approaches to describing and classifying risks (Baccarini et al., 2004). PMBoK (PMI, 2008) suggests the following steps in the risk management process: risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk response planning, and risk monitoring and control. Because risks vary in nature, severity, and consequences, it is important to identify, understand, and manage high-level risks (Baccarini et al., 2004).

The process of identifying and estimating system risks can be accomplished by a variety of techniques—regression analysis, expert systems, and stochastic models (Houston et al., 2001); Influence Diagrams, Monte Carlo Simulation, PERT, Sensitivity Analysis, Multiple Criteria Decision Making (MCDM), Fuzzy Sets Approach (FSA), Neural Networks, Decision Tree And

Fault Tree Analysis, Risk Checklist, Risk Map, Cause-And-Effect Diagram, Delphi Technique, and Combination of Decision Tree and AHP (Dey & Ogunlana, 2004)—which are not addressed in this research.

The approaches to risk management in software projects include the Capability Maturity Model Integration (CMMI) developed by the Software Engineering Institute (SEI 2006); the Rational Unified Process (RUP) (IBM, 2003); the Microsoft Solutions Framework (MSF) (Microsoft, 2002); the AS/NZS 4360 standard (Standards Australia & Standards New Zealand, 2004); the ISO/IEC 15504-5 standard (ISO, 1999); Boehm's list of software risk items (Boehm, 1988); and the ISO 10006 guidelines ((ISO, 2003). Gusmão (2007) presents the chronology of the approaches that address risk management in software projects (Figure 2) up to the year 2001, which have been supplemented by more recent approaches such as MPS.BR (SOFTEX, 2006) and ISO 31000 (ISO, 2009).

Thus, the main approaches were compared (Neves et al., 2014) in order to facilitate the visualization of the steps comprising risk management in software development projects (Chart 1). The comparison was based on the steps of the project risk management knowledge area, described by the PMBoK Guide (PMI, 2008), plus the steps of “solving risks”, “communicating risks”, and “learning”, taken from other approaches (Microsoft, 2002; Standards Australia & Standards New Zealand, 2004).

As can be seen from Chart 1, the various risk management approaches are very similar in their context. Some of these approaches address the steps in more detail, such as PMBoK (PMI, 2008) and CMMI (SEI, 2006), but through examining the context, we perceive that the other approaches do so implicitly. Next, we present the survey data collected for the present study.

## 4 Data survey

Figure 3 displays the results from consultations of CAPES journals in the following databases: Science Direct, Emerald, Wiley, Springer, Wilson, IEEE, and Informs. We used predefined search terms: “risk and project”, “risk and software”, and “risk and incubated technology-based companies”, and searched the major journals on project management, software development, and micro and small businesses. The analysis period extended from the launch date of each journal until September 7, 2009.

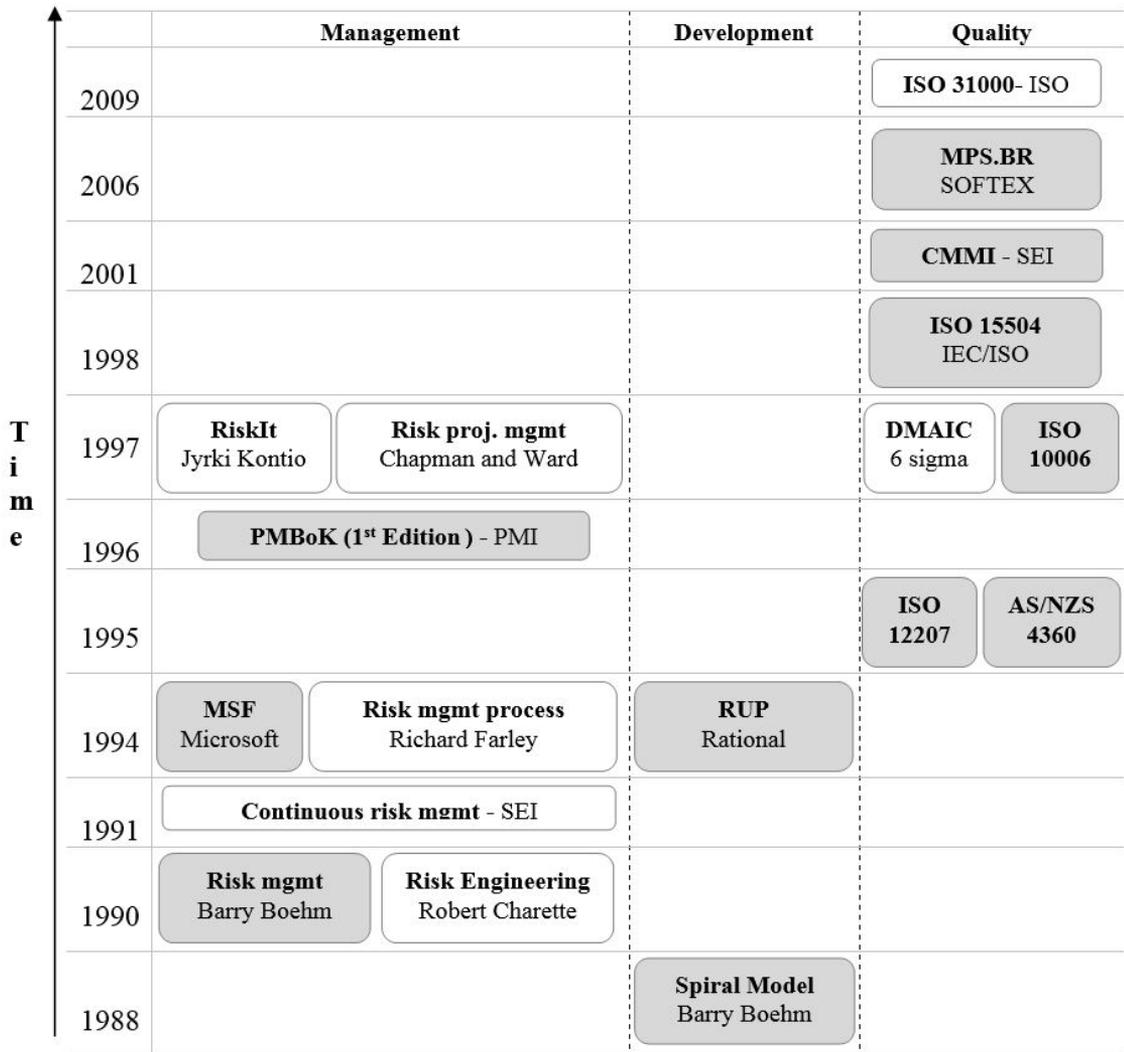


Figure 2. Distribution of publications per focus. Source: Gusmão (2007), supplemented by the authors.

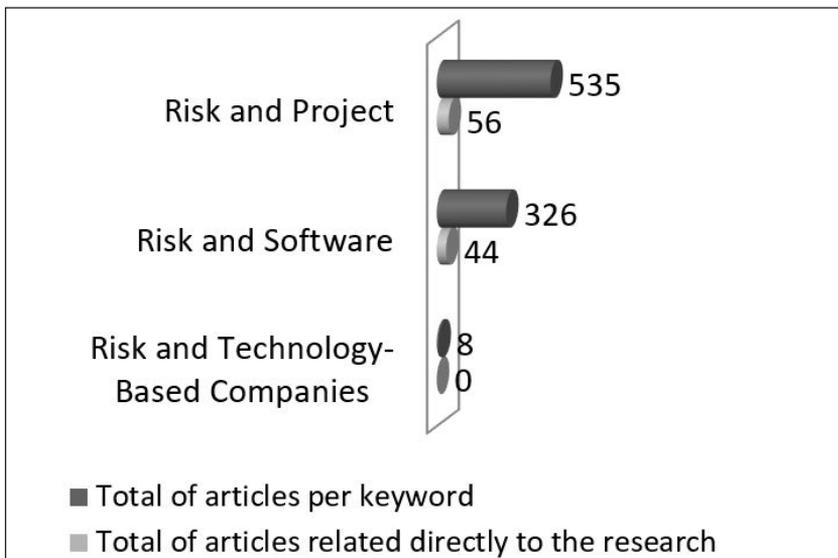


Figure 3. Number of journals corresponding to selected searches.

**Chart 1.** Comparison of approaches to risk management in software projects.

Steps	Boehm (1988)	ISO/IEC 15.504 (1999)	MSF (2002)	RUP (2003)	ISO 10006 (2003)	AS/NZS 4360 (2004)	CMMI (2006)	MPS. BR (2006)	PMBOK (2008)
Risk management Plan		✓	✓	✓		✓	✓	✓	✓
Risk identification	✓	✓	✓	✓	✓	✓	✓	✓	✓
Preparation of qualitative risk analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓
Preparation of quantitative risk analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risk response Plan	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risk solving	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risk monitoring and control	✓	✓	✓	✓	✓	✓	Implicit	✓	✓
Risk reporting			Implicit		Implicit	✓	Implicit		Implicit
Learning			✓		Implicit	Implicit	Implicit		Implicit

Source: Neves et al. (2014).

**Chart 2.** List of journals according to selected searches.

Journals		
Decision Science	IEEE Transactions on Software Engineering	Journal of Management Information Systems
Decision Support Systems	IEEE Transactions on Systems	Journal of Systems and Software
IEEE Computer	Industrial Management & Data Systems	Software Engineering Journal
IEEE Security & Privacy	Information & Management	Software Maintenance: Research and Practice
IEEE Software	Information Management & Computer Security	Technovation
IEEE Spectrum	Information and Software Technology	
IEEE Transactions on Engineering Management	Information Systems Research	

Using the search term “risk and incubated technology-based companies,” few results were obtained, and after examining these individually they were found to be not directly relevant to the subject of this research. Next, we evaluated the 326 articles found under “risk and software,” out of which 44 were selected as being relevant. The journals where the selected items were found can be seen in Chart 2.

Figure 4 shows the main databases referring to the journals.

To provide more current data, the articles were sorted by decade, and the most recent period corresponded to 27 articles (Figure 5).

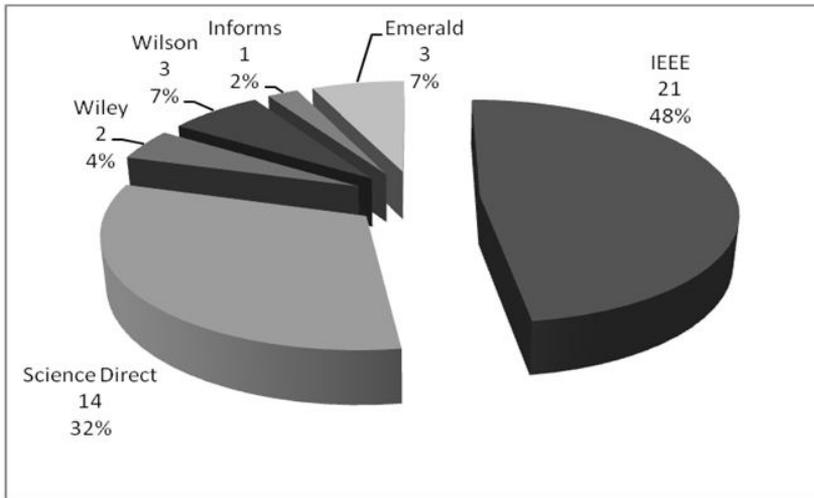
After the selection according to decade, the articles were analyzed and classified.

## 5 Analysis and results

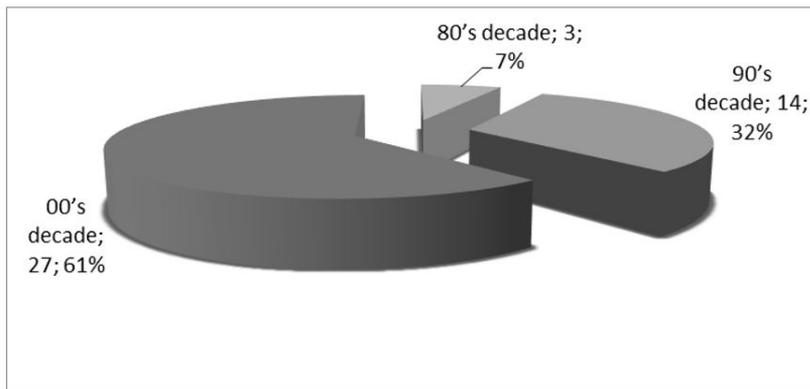
Chart 3 shows a selection of the main results of research about risk management in software projects, based on the articles analyzed.

It was observed that most research efforts have been focused on large public and private enterprises, or members of institutes such as the PMI. Incubated technology-based companies have not been directly cited in the evaluated articles.

In order to classify the research work, we used the data presented in Chart 4 as a reference.



**Figure 4.** Databases surveyed.



**Figure 5.** Percentage distribution of the number of publications per decade.

**Chart 3.** Research on risk management in software projects.

Object of study	Research focus/ Results
Ropponen & Lyytinen (2000)	
83 project managers of the Finnish Information Processing Association (FIPA)	6 main <b>risk components</b> in software found. Principal Component Analysis (PCA) used to reduce the number of items. 1100 projects included.
Jiang et al. (2001)	
194 project managers of the Project Management Institute (PMI)	Development of a <b>model</b> that relates the sources of risk and strategies for success. Finding that organizations are more likely to have a successful project when they are able to minimize the known risks with appropriate strategies.
Schmidt et al. (2001)	
41 project managers of organizations in Hong Kong (9), Finland (13), and the USA (19)	53 <b>risk items</b> grouped into 14 categories. Identification of the most significant risk factors for software development projects. Although there is a substantial area of agreement across different cultures with respect to what some of the main risks are, there are also discernible differences in the identification and understanding of the importance of some risks.
Houston et al. (2001)	
1) 36 software project managers from 22 organizations; 2) 458 managers	<b>Approach</b> to modelling risk factors and simulating its effects as a way of supporting risk management activities in software development.

Chart 3. Continued...

Object of study	Research focus/ Results
Boehm & Turner (2003)	
Software company (Supply Chain)	<b>Method</b> using risk analysis. Use of five-step process to determine the best approach to the project: whether based on agile methods (Scrum, Extreme Programming, Agile software), on plan-driven methods (e.g., Capability Maturity Model, CMM), or on a structure of unified processes complementing one another in a balanced way, so that together they can reduce failures.
Barros et al. (2004)	
2 software projects of two large Brazilian companies	<b>Approach</b> that allows developing, recovering, and reusing the knowledge of and experience in project management through scenarios used to model risk impact and resolution strategies.
Wallace et al. (2004a)	
507 software project managers, members of the Information Systems Special Interest Group (ISSIG) of the Project Management Institute (PMI)	6 <b>risk dimensions</b> presented. Introduction of a <b>conceptual model</b> . Empirical evidence that the most prominent of the risks associated with high-risk projects differ from those of medium and low-risk projects. For high-risk projects, requirements, planning and risk control, and organizational risk are the most prominent risks, while in low-risk projects project complexity is the most prominent.
Baccarini et al. (2004)	
18 managers of IT projects for Australian public and private companies	Identified 27 key <b>risk factors</b> from the literature. Top 10 risk factors ranked in terms of likelihood and consequence, and suggested treatment.
Charette (2005)	
Unsuccessful projects of large companies	Considerations on why software projects <b>fail</b> and the implications.
Costa et al. (2007)	
34 project managers and 16 analysts (11 academic, and 39 corporate from 26 companies)	Risk assessment technique for software projects based on an economic view of the elements of <b>risk factors</b> for these projects. 211 questions classified into 10 risk factors.
Dey et al. (2007)	
Software projects of a public sector organization in Barbados	Development of a seven-step <b>framework</b> for managing risks in software projects from the developers' perspective.
Na et al. (2007)	
3 large Korean software development companies	Developing and testing a risk-based <b>model</b> that simultaneously measures objective (quantitative: cost, time, etc.) and subjective (the performance of the people involved) software performance in IT in developing countries. 3 <b>conceptual models</b> developed. 11 tried and tested hypotheses.
Du et al. (2007)	
118 IT specialists and 140 beginners (students)	Empirical investigation of specific conditions influencing <b>IT risk perception</b> and the subsequent decision to continue a troubled project. Focus on three elements: tools, individual competence, and perceived control. Hypotheses tested via factorial analysis.
Han & Huang (2007)	
115 project managers	6 <b>risk dimensions</b> - 27 risk factors. Selected top 10 risk factors according to 115 software projects evaluated, evaluating their probability of occurrence and level of impact. The "requirement" risk dimension was the one most affecting the performance of the projects evaluated.

**Chart 3.** Continued...

Object of study	Research focus/ Results
Keil et al. (2008)	
149 software development professionals from 4 medium to large companies	Tested hypothesis proved that software practitioners who use a <b>risk checklist</b> are expected to identify more risks than those who do not. Suggested that in the absence of a risk checklist, software practitioners are better able to distinguish between risks that are really there and risks that are not. The checklist can also prompt professionals to see risks that are not really there. The potential value of risk checklists is helping to identify risks that might otherwise go unnoticed.
Emam & Koru (2008)	
IT department project managers. Total in 2005 = 232 Total in 2007 = 156	Estimated software project cancellation rates and the performance of projects that weren't cancelled. Project cancellations: 15.52% in 2005 and 11.54% in 2007.
Huang & Han (2008)	
97 project managers	Through cluster analysis, the results showed that risk exposure associated with the <b>risk dimensions</b> related to "user", "requirement", "planning and control", and "team" were affected by <b>project duration</b> , but also showed how to effectively manage software risks by observing trends in the risk components.
Bannerman (2008)	
23 project managers of government agencies in Australia	Identified 10 major risk factors and 4 distinct project types (pure project form, hybrid form, operational activity, and breakthrough event). Found that risk management practices lag behind project management practices.
Nakatsu & Iacovou (2009)	
57 IT project managers, members of the PMI	Assessed main <b>risk factors</b> of outsourced software development (domestic and offshore) using the Delphi method.

**Chart 4.** Classification of research.

Item	Description	Reference
Place	Country where surveys were conducted	-
Focus	Information about the research focus (main subject)	-
Research method	Articles were catalogued and classified according to the technical procedures used, i.e. "theoretical-conceptual", "simulation", "theoretical modelling", survey", "case study", "action research" and "experimental research"	Bertrand & Fransoo (2002), Gil (2009), Yin (2009), Bryman & Bell (2007), Miguel (2007), Miguel et al. (2009)
Objective	"Exploratory", "descriptive", and "Explanatory"	Gil (2009), Bryman & Bell (2007)
Approach	"Qualitative", "Quantitative", and "Combined"	Creswell & Plano Clark (2007), Bryman & Bell (2007)
Authors' affiliation	"University", "Research Center", and "Company"	-

Next, we present the main results, which in addition to the abstracts presented in Chart 3 include works published by Wallace et al. (2004b), Li et al. (2008), Verdon & McGraw (2004), Barki et al. (2001), Zhou et al. (2008), Sanders & Kelly (2008), Keil et al. (2000) and Kwak & Stoddard (2004).

Figure 6 shows the result of the classification of articles by the place where the research was performed.

Most studies were performed in the United States (45%), and only two in Brazil (7%).

Figure 7 shows the concentration of articles in accordance with the focus of research.

The focus of research shows a trend in the literature toward the analysis of risk factors or risk taxonomies. According to Prieto-Diaz (2002), whereas taxonomy is a categorized structure, classification is the act of assigning entities to the categories defined in the taxonomy. It is the grouping of similar items, based on established criteria. Many authors emphasize the question of risk factors in the literature (McFarlan, 1981; Boehm, 1991; Barki et al., 1993; Sumner,

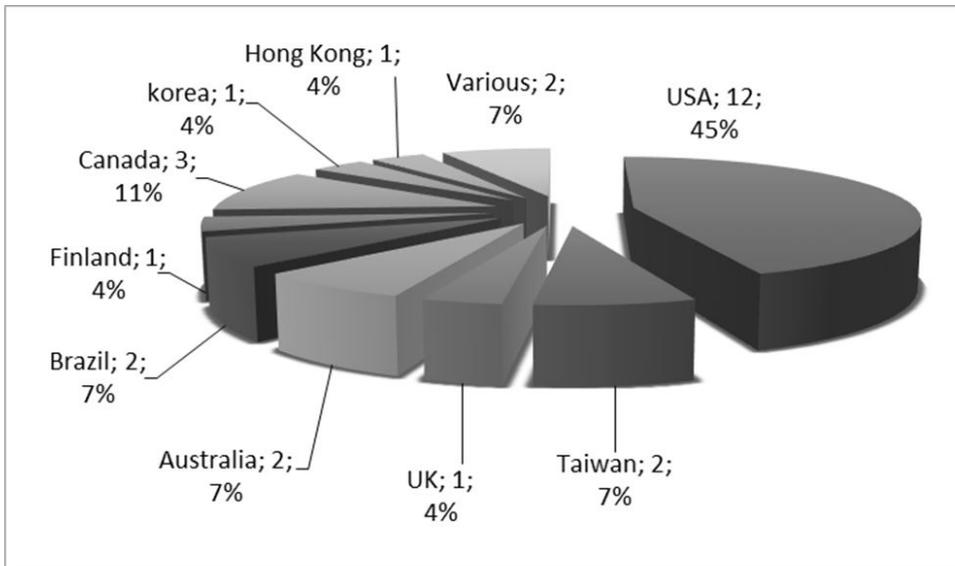


Figure 6. Distribution of publications by location.

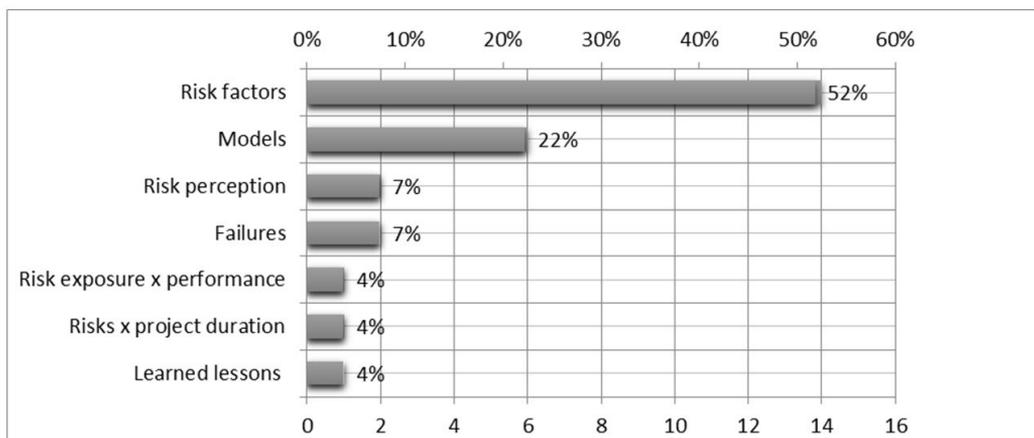


Figure 7. Distribution of publications by research focus.

2000; Longstaff et al., 2000; Cule et al., 2000; Kliem, 2000; Schmidt et al., 2001; Houston et al., 2001; Murthi, 2002; Addison, 2003; Wallace et al., 2004a; Charette, 2005; Han & Huang, 2007; Keil et al., 2008; Bannerman, 2008).

In this regard, Schmidt et al. (2001, p. 7) define risk factor as “[...] a condition that can present a serious threat to the successful completion of a software development project [...]”. The advocates of risk management in software projects suggest that project managers should identify and control these factors to reduce the chance of project failure (Wallace et al., 2004a). Understanding the nature of the different risks involved in the software development process, as well as their relationship to project performance, has become very important, since the plan and the

strategy for risk management strategy depend on it (Han & Huang, 2007). According to Keil et al. (2008), although these risks present variations in the degree of consistency and coverage of the risk domain, there are also similarities in issues such as lack of senior management support, uncertainty about requirements, and lack of user involvement.

However, some criticisms of risk factors or similar approaches are presented in the literature. Murthi (2002) posits that risk taxonomies can be used as guides to project teams in the identification stage of risk management. However, despite the large amount of work done to develop these taxonomies, they tend to ignore the risks that usually affect current projects. Rovai (2005) understands that whereas the advantage of building a list of risks is

that risk identification becomes quick and simple, the disadvantage is that building a comprehensive list of risks is difficult, and the user is effectively limited to the categories in the list.

Figure 8 presents the publications found according to research methods

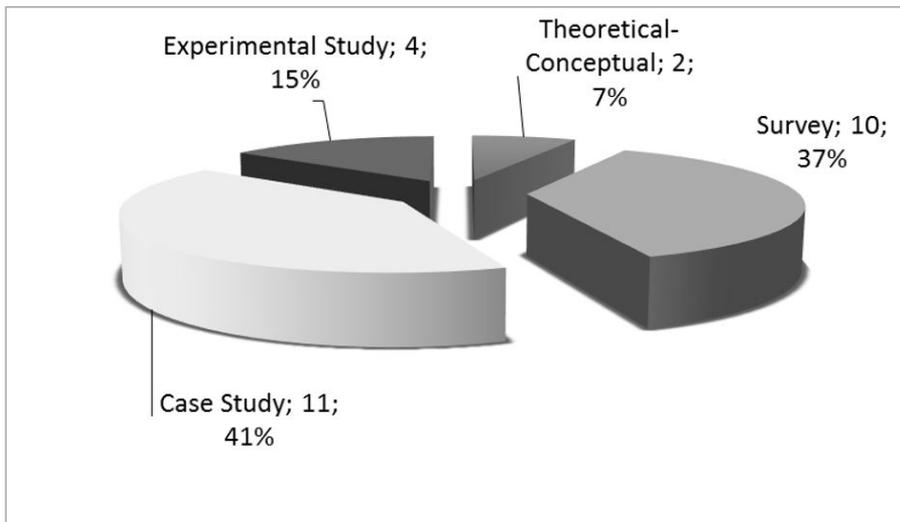
Most research methods fall into two categories: case studies (41%) and surveys (37%), the latter being the most widely-used research method in the United States.

Figure 9 shows research classification according to purpose.

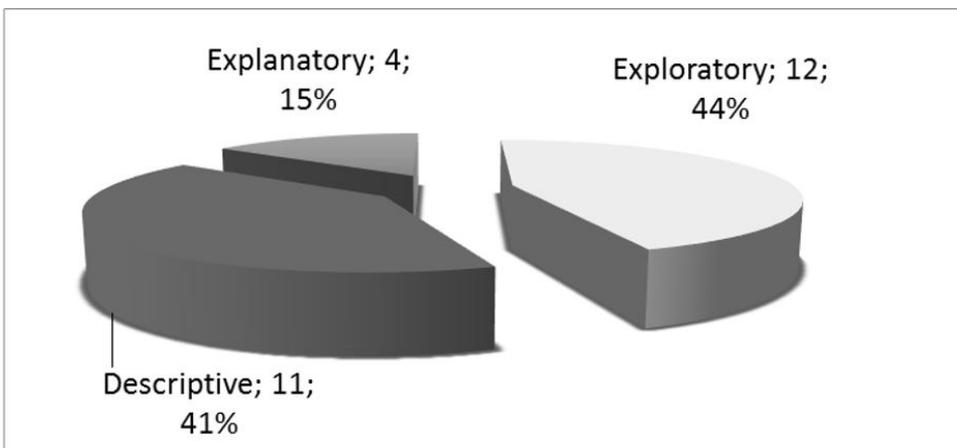
Regarding the distribution of the publications according to the approach used, 56% correspond to qualitative research (Figure 10).

Most researchers of risk management in the software development process—85%—come from universities (Figure 11).

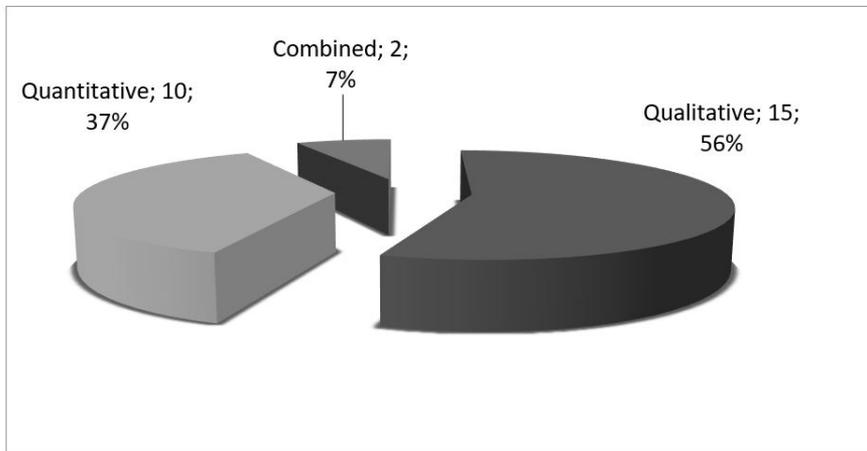
Lastly, we performed a bibliometric analysis to find which of the main articles about risks and software projects were most cited, across all time periods and considering the total number of citations received by the original document. Bibliometrics provides an essentially objective quantitative measure of scientific output (Okubo, 1997). The main source of information for this research was the Institute for Scientific Information's (ISI) Web of Science database, which comprises three citation indices: the Science Citation Index (SCI), the Social Science Citation Index (SSCI), and the Arts and Humanities Citation Index (AHCI), the last one being disregarded for this study.



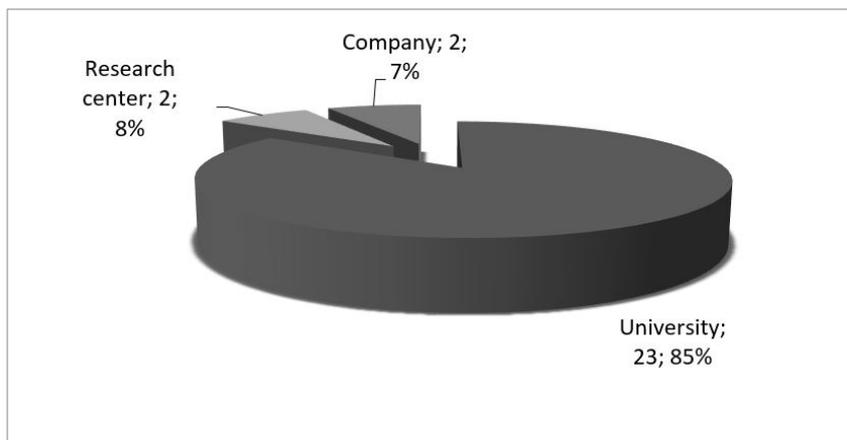
**Figure 8.** Distribution of publications by research method.



**Figure 9.** Distribution of publications by purpose.



**Figure 10.** Distribution of publications by approach.



**Figure 11.** Distribution of publications by author affiliation.

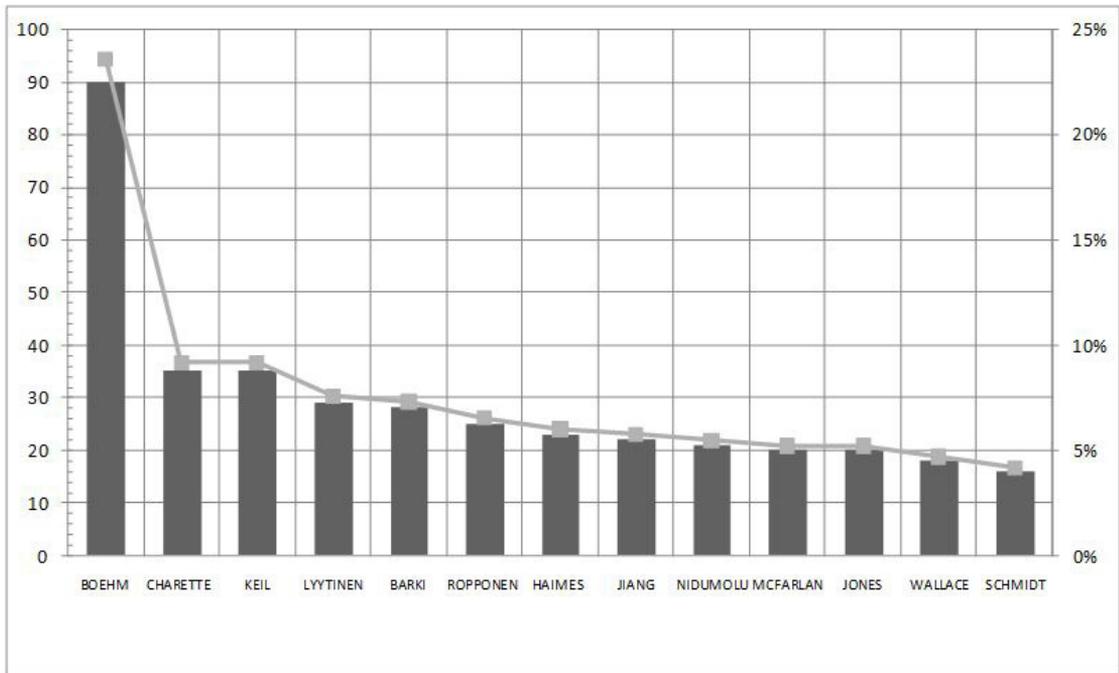
Figure 12 shows the ranking of the most-cited authors, those with over 15 citations.

Data were quantified through the use of the Sitkis and UCINET bibliometric tools, which converted textual information into numerical data in order to allow the completion of the statistical analyses, generating lists, tables, and matrices. We understand that authors cite articles that are important in the development of their research. Thus, “Boehm”, “Charette”, and “Keil” have been identified as authors with the most citations. Of the 13 most-cited authors we found, 10 were included in this study, indicating the relevance of the selected works. Articles by the authors “Haimes” and “Nidumolu” were not included due to the years of publication (70s, 80s and 90s decades), and nor were those by the author “Jones” because most refer to his 1994 book *Assessment and control of software risks*.

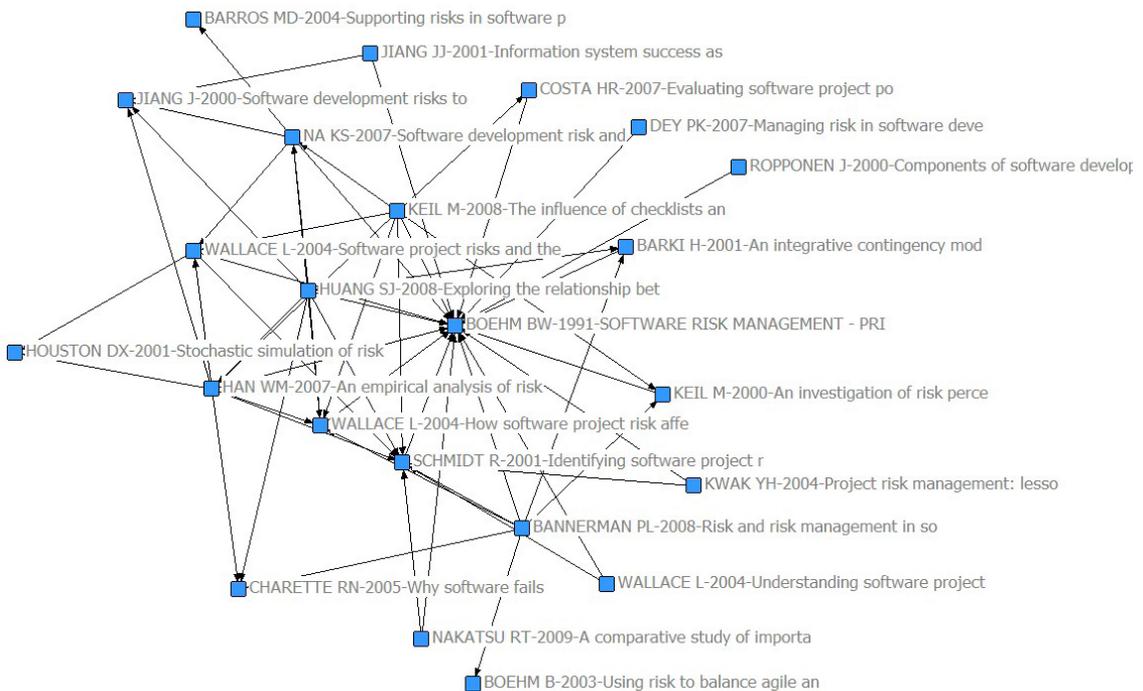
Implementing co-citation analysis of articles allows us to evaluate the citations among pairs so as to realize the similarity between content items. According to Marshakova (1981), co-citation quantifies the relationship between two or more articles, according to the number of documents where they are cited simultaneously. Our analysis considered some of the key research articles, including that of the most cited author, “Boehm” (Figure 13).

All authors can be seen to converge on the 1991 article by “Boehm” 1991, and relationships exist among the other articles.

In order to evaluate the Brazilian scientific production on the topic, we surveyed major journals in Production Engineering (Qualis B2 by CAPES), using the keyword “risks and software” in the “summary/abstract” field. The period of analysis considered the starting date of each journal up to September 7, 2009. The results can be seen in Chart 5.



**Figure 12.** Most commonly cited authors on risks and software projects.



**Figure 13.** Co-citation analysis of main articles.

**Chart 5.** Research in Brazil on risk management and software development projects.

Journals	Total of articles published
Gestão & Produção	0
Produção	0
Pesquisa Operacional	0

It is clear that in Brazil, the topic “risks and software projects” has not been explored for publication in production engineering journals. Even a full search of Brazil’s Scielo database does not return any results for these keywords. However, they are objects of research in Brazilian universities, for example, in the areas of Administration (Leopoldino, 2004), and especially Systems and Computer Engineering (Gusmão, 2007).

## 6 Discussion and conclusions

Because of the relatively small number of articles analysed, it is not possible to generalize our findings, but some the following considerations can be inferred from the study:

- Publications are concentrated in the IEEE database (48%);
- Most researchers are from the USA (45%);
- Research classification was problematic, because articles, especially older ones, did not provide related information. There is a predominance of case studies (41%), followed by surveys (37%) as research methods. Information about the object of study was not clear either;
- Most studies on risk management are still theoretical (academics, 85%) with goals classified as exploratory (44%) or descriptive (41%)—and only 15% explanatory, which corroborates the criticisms that some techniques and practices on risk management which have been proposed in the literature are still little explored in their application and results;
- The most-cited author in the research as evaluated by bibliometric analysis, “Boehm”, can be considered a classic author on the subject of risk management in software projects, being also the author of one of the earliest approaches, the spiral model, shown in Chart 1.

Regarding trends in the literature evaluated, it appears that the studies are primarily focused on identifying risk factors (52%), a recurring theme. However, we perceive that the authors are concerned with establishing both the dynamics of the software development environment, which can quickly outdate the work in this area, and the culture of the country where the study is conducted, which allows the emergence of further studies on this theme. The lack of research on this subject in some journals that focus on research on micro and small enterprises also suggests more studies to be conducted. Another motivating factor for further research in micro and small incubated

technology-based companies is that, in most cases, the objects of study referred to large companies or projects in the public and private sector; none of the studies assessed mentioned incubated companies. Identifying and classifying risks in a incubated company may represent a breakthrough in their management processes, enabling new research that may help the managers of these companies to assess which activities need more attention regarding potential risks, and what decisions to make if the situation should occur.

## Acknowledgements

We are grateful to CAPES and FAPEMIG for proving the funding that has enabled this research.

## References

- Addison, T. (2003) E-commerce project development risks: evidence from a Delphi survey. *International Journal of Information Management*, 23(1), 25-40. [http://dx.doi.org/10.1016/S0268-4012\(02\)00066-X](http://dx.doi.org/10.1016/S0268-4012(02)00066-X).
- Associação para Promoção da Excelência do Software Brasileiro – SOFTEX. (2006). *Melhoria de processo do software brasileiro, versão 1.1*. Brasília: Softex. Recuperado em 19 de setembro de 2009, de [www.softex.br](http://www.softex.br)
- Baccarini, D., Salm, G., & Love, P. E. D. (2004). Management of risks in information technology projects. *Industrial Management & Data Systems*, 104(4), 286-295. <http://dx.doi.org/10.1108/02635570410530702>.
- Bannerman, P. L. (2008). Risk and risk management in software projects: a reassessment. *Journal of Systems and Software*, 81(12), 2118-2133. <http://dx.doi.org/10.1016/j.jss.2008.03.059>.
- Barki, H., Rivard, S., & Talbot, J. (1993). Toward an assessment of software development risk. *Journal of Management Information Systems*, 10(2), 203-225. <http://dx.doi.org/10.1080/07421222.1993.11518006>.
- Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems*, 17(4), 37-69.
- Barros, M. O., Werner, C. M. L., & Travassos, G. H. (2004). Supporting risks in software project management. *Journal of Systems and Software*, 70(1-2), 21-35. [http://dx.doi.org/10.1016/S0164-1212\(02\)00155-3](http://dx.doi.org/10.1016/S0164-1212(02)00155-3).
- Bertrand, J. W. M., & Fransoo, J. C. (2002). Modeling and simulation: operations management research methodologies using quantitative modeling. *International Journal of Operations & Production Management*, 22(2), 241-264. <http://dx.doi.org/10.1108/01443570210414338>.
- Boehm, B. W. (1988). A spiral model of software development and enhancement. *IEEE Computer*, 21(5), 61-72. <http://dx.doi.org/10.1109/2.59>.
- Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE Software*, 8(1), 32-41. <http://dx.doi.org/10.1109/52.62930>.

- Boehm, B., & Turner, R. (2003). Using risk to balance agile and plan-driven methods. *IEEE Computer*, 36(6), 57-66. <http://dx.doi.org/10.1109/MC.2003.1204376>.
- Brasil. Ministério da Ciência, Tecnologia e Inovação. Secretaria de Política de Informática – SEPIN. (2002). *Qualidade e Produtividade no Setor de Software Brasileiro*. Brasília: Ministério da Ciência e Tecnologia. Recuperado em 13 de fevereiro de 2010, de <http://www.mct.org.br>
- Bryde, D. J. (2003). Project management concepts, methods and application. *International Journal of Operations & Production Management*, 23(7), 775-793. <http://dx.doi.org/10.1108/01443570310481559>.
- Bryman, A., & Bell, E. (2007). *Business research methods* (2 ed.). New York: Oxford University Press.
- Carnevali, J. A., & Miguel, P. A. C. (2007). Revisão, análise e classificação da literatura sobre o QFD – tipos de pesquisa, dificuldades de uso e benefícios do método. *Gestão & Produção*, 14(3), 557-579. <http://dx.doi.org/10.1590/S0104-530X2007000300011>.
- Charette, R. N. (2005). Why software fails. *IEEE Spectrum*, 42(9), 42-49. <http://dx.doi.org/10.1109/MSPEC.2005.1502528>.
- Costa, H., Barros, M. O., & Travassos, G. H. (2007). Evaluating software project portfolio risks. *Journal of Systems and Software*, 80(1), 16-31. <http://dx.doi.org/10.1016/j.jss.2006.03.038>.
- Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*, California: Sage Publications.
- Cule, P., Schmidt, R., Lyytinen, K., & Keil, M. (2000). Strategies for heading off IS project failure. *Information Systems Management*, 17(2), 65-73. <http://dx.doi.org/10.1201/1078/43191.17.2.20000301/31229.8>.
- Dahlstrand, A. L. (2007). Technology-based entrepreneurship and regional development: the case of Sweden. *European Business Review*, 19(5), 373-386. <http://dx.doi.org/10.1108/09555340710818969>.
- Dey, P. K., & Ogunlana, S. O. (2004). Selection and application of risk management tools and techniques for Build-operate-transfer Projects. *Industrial Management & Data Systems*, 104(4), 334-346. <http://dx.doi.org/10.1108/02635570410530748>.
- Dey, P. K., Kinch, J., & Ogunlana, S. O. (2007). Managing risk in software development projects: a case study. *Industrial Management & Data Systems*, 107(2), 284-303. <http://dx.doi.org/10.1108/02635570710723859>.
- Du, S., Keil, M., Mathiassen, L., Shen, Y., & Tiwana, A. (2007). Attention-shaping tools, expertise, and perceived control in IT project risk assessment. *Decision Support Systems*, 43(1), 269-283. <http://dx.doi.org/10.1016/j.dss.2006.10.002>.
- Emam, K. E., & Koru, A. G. (2008). A replicated survey of IT software project failures. *IEEE Software*, 25(5), 84-90. <http://dx.doi.org/10.1109/MS.2008.107>.
- Gil, A. C. (2009). *Como elaborar projetos de pesquisa* (4 ed.). São Paulo: Atlas.
- Gusmão, C. M. G. (2007). *Um modelo de processo de gestão de riscos para ambientes de múltiplos projetos de desenvolvimento de software* (Tese de doutorado), Centro de Informática, Universidade Federal de Pernambuco, Recife.
- Han, W.-M., & Huang, S.-J. (2007). An empirical analysis of risk components and performance on software projects. *Journal of Systems and Software*, 80(1), 42-50. <http://dx.doi.org/10.1016/j.jss.2006.04.030>.
- Houston, D., Mackulak, G., & Collofello, J. (2001). Stochastic simulation of risk factor potential effects for software development risk management. *Journal of Systems and Software*, 59(3), 247-257. [http://dx.doi.org/10.1016/S0164-1212\(01\)00066-8](http://dx.doi.org/10.1016/S0164-1212(01)00066-8).
- Huang, S.-J., & Han, W.-M. (2008). Exploring the relationship between software project duration and risk exposure: A cluster analysis. *Information & Management*, 45(3), 175-182. <http://dx.doi.org/10.1016/j.im.2008.02.001>.
- International Business Machines – IBM. Rational Software Corporation. (2003). *Rational unified process: best practices for software development teams* (Rational Software White Paper, TP026B, Rev 11/01: IBM). Cupertino, CA: Rational Software Corporation. Recuperado em 12 de setembro de 2009, de <http://www.ibm.com/developerworks/rational/library>
- International Organization for Standardization – ISO. (1999). *ISO/IEC 15.504-5:1999 – Information technology - Software process assessment — Part 5: An assessment model and indicator guidance*. Genebra: ISO.
- International Organization for Standardization – ISO. (2003). *ISO 10.006:2003 - quality management systems - guidelines for quality management in projects*. Genebra: ISO.
- International Organization for Standardization – ISO. (2009). *ISO 31.000:2009 - risk management - principles and guidelines on implementation*. Genebra: ISO. Recuperado em 21 setembro de 2009, de [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=43170](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170)
- Jiang, J. J., Klein, G., & Discenza, R. (2001). Information System Success as Impacted by Risks and Development Strategies IEEE. *Transactions on Engineering Management*, 48(1), 46-55. <http://dx.doi.org/10.1109/17.913165>.
- Keil, M., Li, L., Mathiassen, L., & Zheng, G. (2008). The influence of checklists and roles on software practitioner risk perception and decision-making. *Journal of Systems and Software*, 81(6), 908-919. <http://dx.doi.org/10.1016/j.jss.2007.07.035>.
- Keil, M., Wallace, L., Turk, D., Dixon-Randall, G., & Nulden, U. (2000). An investigation of risk perception and risk propensity on the decision to continue a software development project. *Journal of Systems and*

- Software*, 53(2), 145-157. [http://dx.doi.org/10.1016/S0164-1212\(00\)00010-8](http://dx.doi.org/10.1016/S0164-1212(00)00010-8).
- Kendrick, T. (2003). *Identifying and managing project risk: essential tools for failure-proofing your project*. New York: Amacom.
- Kerzner, H. (2006). *Gestão de projetos: as melhores práticas*. Porto Alegre: Bookman.
- Kliem, R. (2000). Risk management for business process reengineering projects. *Information Systems Management*, 17(4), 71-73. <http://dx.doi.org/10.1201/1078/43193.17.4.20000901/31256.12>.
- Kwak, Y. H., & Stoddard, J. (2004). Project risk management: lessons learned from software development environment. *Technovation*, 24(11), 915-920. [http://dx.doi.org/10.1016/S0166-4972\(03\)00033-6](http://dx.doi.org/10.1016/S0166-4972(03)00033-6).
- Lahorgue, M. A., & Hanefeld, A. O. (2004). A localização das incubadoras tecnológicas no Brasil: reforço ou quebra da tendência histórica de concentração das infra-estruturas de ciência, tecnologia e inovação. *Estudos do CEPE (UNISC)*, 19, 7-21.
- Leopoldino, C. B. (2004). *Avaliação de riscos em desenvolvimento de software* (Dissertação de mestrado). Universidade Federal do Rio Grande do Sul, Porto Alegre.
- Li, J., Conradi, R., Slyngstad, O. P. N., Torchiano, M., & Morisio, M. (2008). A state-of-the-practice survey of risk management in development with off-the-shelf software components. *IEEE Transactions on Software Engineering*, 34(2), 271-286. <http://dx.doi.org/10.1109/TSE.2008.14>.
- Longstaff, T. A., Chittister, C., Pethia, R., & Haimes, Y. Y. (2000). Are we forgetting the risks of information technology? *IEEE Computer*, 33(12), 43-51. <http://dx.doi.org/10.1109/2.889092>.
- Marshakova, I. V. (1981). Citation networks in information science. *Scientometrics*, 31(1), 13-16. <http://dx.doi.org/10.1007/BF02021861>.
- McFarlan, F. (1981). Portfolio approach to information systems. *Harvard Business Review*, 59(5), 142-150.
- Microsoft. (2002). *Microsoft Solutions Framework: MSF Risk Management Discipline v. 1.1*. Recuperado em 18 de setembro de 2009, de <http://www.microsoft.com/msf>
- Miguel, P. A. C. (2007). Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução. *Produção*, v. 17, n. 1, p. 216-229. <http://dx.doi.org/10.1590/S0103-65132007000100015>.
- Miguel, P. A. C., Fleury, A., Mello, C. H. P., Nakano, D. N., Turrioni, J. B., Ho, L. L., Martins, R. A., Pureza, V. M. M., & Morabito, R. (2009). *Metodologia de pesquisa em engenharia de produção e gestão de operações*. Rio de Janeiro: Elsevier.
- Murphy, A., & Ledwith, A. (2007). Project management tools and techniques in high-technology SMEs. *Management Research News*, 30(2), 153-166. <http://dx.doi.org/10.1108/01409170710722973>.
- Murthi, S. (2002). Preventive risk management for software projects. *IT Professional*, 4(5), 9-15. <http://dx.doi.org/10.1109/MITP.2002.1041172>.
- Na, K.-S., Simpson, J. T., Li, X., Singh, T., & Kim, K.-Y. (2007). Software development risk and project performance measurement: evidence in Korea. *Journal of Systems and Software*, 80(4), 596-605. <http://dx.doi.org/10.1016/j.jss.2006.06.018>.
- Nakatsu, R. T., & Iacovou, C. L. (2009). A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: a two-panel Delphi study. *Information & Management*, 46(1), 57-68. <http://dx.doi.org/10.1016/j.im.2008.11.005>.
- Neves, S. M., Silva, C. E. S., Salomon, V. A. P., Silva, A. F., & Sotomonte, B. E. P. (2014). Risk management in software projects through Knowledge Management techniques: cases in Brazilian Incubated Technology-Based Firms. *International Journal of Project Management*, 32(1), 125-138.
- Okubo, Y. (1997). *Bibliometric indicators and analysis or research systems: methods and examples*. Paris: OCDE.
- Pinna, C. C. A., & Carvalho, M. M. (2008). Gestão de escopo em projetos de aplicações web. *Revista Produção OnLine*, v. 8, n. 1, p. 1-8. <http://dx.doi.org/10.14488/1676-1901.v8i1.25>.
- Prieto-Díaz, R. (2002). A faceted approach to building ontologies. In *Proceedings of the 21st International Conference on Conceptual Modeling-ER2002* (pp. 1-18). Tampere, Finland. Recuperado em 12 de setembro de 2009, de <http://www.cs.uu.nl/docs/vakken/ks/0809/BulidOntologiesRPD-ER2002.pdf>
- Project Management Institute – PMI. (2008). *A guide to the Project Management Body of Knowledge (PMBok® Guide)*. Pennsylvania: PMI.
- Raz, T., Shenhar, A. J., & Dvir, D. (2002). Risk management, project success, and technological uncertainty. *R & D Management*, 32(2), 101-109. <http://dx.doi.org/10.1111/1467-9310.00243>.
- Ropponen, J., & Lyytinen, K. (2000). Components of software development risk: how to address them? A project manager survey. *IEEE Transactions on Software Engineering*, 26(2), 98-112. <http://dx.doi.org/10.1109/32.841112>.
- Rovai, R. L. (2005). *Modelo para gestão de riscos em projetos: estudo de múltiplos casos* (Tese de doutorado). Escola Politécnica, Universidade de São Paulo, São Paulo.
- Saarinen, T. (1996). An expanded instrument for evaluating information system success. *Information & Management*, 31(2), 103-118. [http://dx.doi.org/10.1016/S0378-7206\(96\)01075-0](http://dx.doi.org/10.1016/S0378-7206(96)01075-0).

- Sanders, R., & Kelly, D. (2008). Dealing with risk in scientific software development. *IEEE Software*, 25(4), 21-28. <http://dx.doi.org/10.1109/MS.2008.84>.
- Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: an international delphi study. *Journal of Management Information Systems*, 17(4), 5-36.
- Software Engineering Institute – SEI. (2006). *CMMI® for development. staged representation, version 1.2, technical report (06tr008)*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University. Recuperado em 12 de setembro de 2009, de <http://www.sei.cmu.edu/reports/06tr008.pdf>
- Standards Australia & Standards New Zealand. (2004). *AS/NZS 4360:2004: risk management*. Sydney: Standards Australia; Standards New Zealand.
- Sumner, M. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of Information Technology*, 15(4), 317-327. <http://dx.doi.org/10.1080/02683960010009079>.
- The Standish Group. (2000). *Extreme chaos*. Recuperado em 13 de julho de 2009, de [www.standishgroup.com/sample\\_research/PDFpages/extreme\\_chaos.pdf](http://www.standishgroup.com/sample_research/PDFpages/extreme_chaos.pdf)
- Verdon, D., & McGraw, G. (2004). Risk analysis in software design. *IEEE Security and Privacy*, 2(4), 79-84. <http://dx.doi.org/10.1109/MSP.2004.55>.
- Wacker, J. G. (2004). A theory of formal conceptual definition: developing theory-building measurement instruments. *Journal of Operations Management*, 22(6), 629-650. <http://dx.doi.org/10.1016/j.jom.2004.08.002>.
- Wallace, L., Keil, M., & Rai, A. (2004a). Understanding software project risk: a cluster analysis. *Information & Management*, 42(1), 115-125. <http://dx.doi.org/10.1016/j.im.2003.12.007>.
- Wallace, L., Keil, M., & Rai, A. (2004b). How software project risk affects project performance: an investigation of the dimensions of risk and an exploratory model. *Decision Sciences*, 35(2), 289-321. <http://dx.doi.org/10.1111/j.00117315.2004.02059.x>.
- White, D., & Fortune, J. (2002). Current practice in project management - an empirical study. *International Journal of Project Management*, 20(1), 1-11. [http://dx.doi.org/10.1016/S0263-7863\(00\)00029-6](http://dx.doi.org/10.1016/S0263-7863(00)00029-6).
- Yin, R. K. (2009). *Case study research: design and methods* (4 ed.). Thousand Oaks: Sage Publications, Inc.
- Zhou, L., Vasconcelos, A., & Nunes, M. (2008). Supporting decision making in risk management through an evidence-based information systems project risk checklist. *Information Management & Computer Security*, 16(2), 166-186. <http://dx.doi.org/10.1108/09685220810879636>.