Indicators and Metrics for Risk Assessment in Software Projects: A Mapping Study

Júlio Menezes Jr.¹, Cristine Gusmão² and Hermano Moura¹

¹ Centro de Informática, Universidade Federal de Pernambuco, Recife, Pernambuco, Brasil
{jvmj, hermano}@cin.ufpe.br

² Departamento de Cirurgia, Núcleo de Telessaúde, Universidade Federal de Pernambuco, Recife, Pernambuco, Brasil
cristine.gusmao@nutes.ufpe.br

Abstract. The usage of metrics and indicators in software development companies acts in both strategic and tactical levels, it is effective for optimization of processes and also helps in managerial decisions. On the other hand, because of abstractness and subjectivity of the risk, the risk management is many times overlooked by the software development organizations. Therefore, it is necessary the definition of metrics and indicators for risk assessment in order to make the risk management a more reliable activity through real information and data available from projects. In this light, this paper presents the application of a systematic mapping study that aims to raise related work to the usage of metrics and indicators for risk assessment in multiple projects environments.

Keywords. Risk Assessment, Indicators, Systematic Mapping Study.

1 Introduction

The need of software products by the companies in general is perceptible, and it is in many cases essential for their improvement or even their survival. Likewise, organizations that develop software must be aligned to the business models of these companies in order to generate products that meet their needs, commonly inside constraints of cost, time, scope and quality. Faced with these challenges, software development organizations have to manage effectively their projects, under penalty of losing their place in the market because of lack of effective and proactive practices of management. Then, it is necessary to have an organizational structure that allows, for example, the overview of riskier projects, and their control based on information from risks or that indicates risks, providing a better risk-driven management.

In addition, the usage of processes, techniques and tools for risk management is more recognized in software development environments [1, 2]. Some authors consider that managing projects is managing risks [3]. This fact is due, in part, by the understanding that a significant portion of projects failures could be related to a poor risk management. The risk management is one of the disciplines related to project man-
agement, and its usage becomes increasingly necessary as the size and complexity of software grows [4].

Despite the relevance of risk management in software project management, given the diversity of existent approaches, models and processes that deal with software risk management [2, 5, 6, 7], the risk management is still usually overlooked by the organizations that develop software. One reason for this fact is that the concept of risk is abstract and subjective, and its management does not bring apparent immediate practical result [8].

Another problem that inhibits risk management is that it is a relatively recent subject in software project management, and its practical application tends to be biased [6], because there is still a high degree of subjectivity especially during the activity of risk assessment. Differently in the financial market, where the risk management is consolidated and widely applied, it is currently a need for the companies that work in this field [9]. Briefly, risk management practices just became effectively consolidated in the financial market when the uncertainties became measurable. In this light, we can say that there is a lack of indicators and metrics that support risk management in the context and viewpoint of software project management, even when we consider organizational factors.

Inside this context, this work presents a systematic mapping study in order to collect evidences about the existence of metrics and indicators that support risk assessment in project management. This paper allows the identification of related work that helps in the proposition of specific metrics or indicators for multiple software projects environments.

For better understanding, the paper is organized as follows: Section 2 presents the research protocol and methodology of the systematic mapping study; the Section 3 summarizes the results; Section 4 presents the limitations of this work and, finally, the Section 6 concludes the paper and presents future work.

2 Application of Systematic Mapping Study

According to Kitchenham and Charter [10], the usage of systematic mapping studies is appropriate when we want to have an overview of a particular subject or theme. Its objective is to summarize the data that answers the research question, and it commonly does not include statistical analysis or meta-analysis1. Systematic mapping study is recommended when very little evidence is likely to exist or that the topic is very broad, and it usually is the first step for future systematic reviews because the research questions tend to be broader.

It is important to notice that the procedure adopted for systematic mapping study in the phases of planning and execution is the same for systematic reviews. The only difference is the fact that a systematic review presents a deeper quantitative data analysis after the selection of publications. Thus, for conducting this mapping study, the

---

1 Meta-analysis is a kind of a secondary study where the results are summarized quantitatively. It is commonly used in systematic reviews.
technical report of Biolkchini and other authors [11] was adopted as the guide for this systematic mapping study.

One of the initial activities to execute the systematic mapping studies is the protocol definition, which specifies the research questions and the necessary steps to the execution of the study. In the next subsections we present the research protocol adopted for this work.

2.1 Mapping Study Protocol

To define this protocol, the research question focus to be formulated must be clear. The research question is crucial to define the appropriate protocol to the mapping study goals. For this work, the focus of the research question is related to the identification of indicators and metrics that support risk management in the context of software projects, and to find the set of information and data necessary to assist the risks measurement in software project.

It is noteworthy that, despite the focus on software projects, this study also includes organizational and tactical management levels. Thus, the view of management is broader, since we must take into consideration the financial and management aspects and analysis of its application in software development environments. Therefore, we also consider works of the following areas of knowledge: i) Management, because it deals with management at various levels, and ii) Economics, because it is an area in which risk assessment process is performed quantitatively.

2.1.1 Research Question Formulation

This subsection presents i) the objects to be investigated (Research Questions), ii) the subject and area where the object will be studied (Population), iii) at which point of the population the object will be studied (Intervention), and iv) what are the results to be considered (Outcomes). These are the research questions:

Primary – What are the evidences of works that approach metrics and indicators for risk assessment?
Secondary – Based on the evidences found, which information is used to measure risks?

In this research, evidence means any papers published in conferences and journals that bring proposals of metrics, indicators and approaches of risk measurement in general. Our main focus is to find not only metrics and indicators, but also mainly the type of information used to define these measures. Therefore, for each evidence we extracted the type of information that composes each proposal of metric and indicator. We decided to provide a more qualitative analysis of the results because we aimed to use them to propose indicators for risk assessment in environments of software projects with focus on the identification of the type of information and associated risk factors.

Population:
Works related to management and assessment of projects.

Intervention:
Approaches, techniques and methods for risk assessment.
Outcomes:
Approaches of risk measurement, indicators and metrics that support risk management and risk assessment. To answer the secondary question, we added the type of data and information used to measure risks.

2.1.2 Inclusion Criteria
To select papers that address the research questions, criteria must be defined. These are:
- Discuss about metrics and indicators for risk assessment;
- Only full papers. Abstracts only will not be accepted;
- Search strings must appear in the title, abstract or keywords;
- Free or accessible through CAPES portal\(^2\);
- Published since 2004;
- Written in English;
- It must be part of at least one of the following major areas of knowledge: i) Computer Science, ii) Management and iii) Economics.

We just considered more recent works (from 2004) to show how the project management community currently deals with metrics and indicators for risk management. And as project management is multidisciplinary, we considered works from other areas such as management and economics too.

2.1.3 Approach to Select Sources
To source selection, we used as a criterion to choose of the most relevant and used sources in the area of software engineering and project management that allow a reliable search using web search engines. Three sources were selected: i) Scopus (http://www.scopus.com), ii) IEEExplore (http://ieeexplore.ieee.org) and iii) Engineering Village (http://www.engineeringvillage2.org).

2.1.4 Search Strategy
Table 1 summarizes the adopted search strategy.

<table>
<thead>
<tr>
<th>Table 1. Search strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strings</strong></td>
</tr>
<tr>
<td><strong>Population</strong></td>
</tr>
<tr>
<td>&quot;Software project&quot; OR &quot;Project management&quot; OR &quot;Software development project&quot; OR &quot;Project assessment&quot; OR &quot;Project appraisal&quot; OR &quot;Project estimate&quot; OR &quot;Project estimation&quot; OR &quot;Project evaluation&quot; OR &quot;Project valuation&quot;</td>
</tr>
<tr>
<td><strong>Intervention</strong></td>
</tr>
<tr>
<td>&quot;Risk management&quot; OR &quot;Organizational risk&quot; OR &quot;Operational risk&quot; OR &quot;Risk assessment&quot; OR &quot;Software risk management&quot; OR &quot;Project risk&quot; OR &quot;Risk appraisement&quot; OR &quot;Risk estimation&quot; OR &quot;Risk evaluation&quot; OR &quot;Risk valuation&quot; OR &quot;Risk analysis&quot;</td>
</tr>
<tr>
<td><strong>Outcomes</strong></td>
</tr>
<tr>
<td>&quot;Risk measurement&quot; OR &quot;Metric&quot; OR &quot;Metrics&quot; OR &quot;Indicator&quot; OR &quot;Measure&quot; OR &quot;Mensuration&quot;</td>
</tr>
</tbody>
</table>

Search Strategy: Population AND Intervention AND Outcomes

\(^2\)CAPES portal (http://www.periodicos.capes.gov.br/) allows the access of main indexed journals and conference papers in main Brazilian universities.
As shown, to perform searches in the selected sources, we defined a set of keywords to the population, intervention and outcomes. The Boolean operators and the combination between strings are accepted by these sources.

The definition of the research protocol was defined by all the authors, which have theoretical and practical experience in software project management and risk management.

3 Results

This section shows the results found, including the analysis of the selected papers. We found 506 articles using the search strategy presented at Table 1. The Table 2 shows the number of references retrieved from each source using the defined search strategy on papers published in conferences and/or journals from 2004.

<table>
<thead>
<tr>
<th>Source</th>
<th>Number of work found</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scopus</td>
<td>339</td>
</tr>
<tr>
<td>IEEEExplore</td>
<td>49</td>
</tr>
<tr>
<td>Engineering Village</td>
<td>118</td>
</tr>
</tbody>
</table>

Figure 1 summarizes the work done so far through the flow used to papers selection.

Figure 1. Search summarization

Four steps were performed to the study selection, where initially we found 506 papers and at the end, with the application of the inclusion criteria, just 24 were select-
All the selected papers fit to all inclusion criteria presented at Section 2.1.2. To better organize the activities, we followed these steps. In step 1, we just applied the search strategy using the strings and Boolean operators shown in Table 1. The selected sources enable the search of strings on the abstract, title, indexed keywords and the year of publication. In addition, in the Scopus is possible to choose works just from the major areas of Physical and Social Science and Humanities. Considering also duplicated works, 506 papers were returned using the web search engine.

The selection of works from the areas of interest in step 2 involved the elimination of works that do not approach risk assessment in projects in the context of economics, management and computer science and the elimination of duplicates. In this step we just considered works that were free or available through CAPES portal. From 506 papers, 115 were selected.

The step 3 consisted of careful reading of the title, abstract and keywords in order to identify potential works that answer the research questions. We analyzed 115 papers, and 63 were pre-selected for full reading. And finally, in step 4 the full text of the remaining papers was read. After the analysis of 63 articles, only 24 ones brought proposals of measures, metrics or indicators for risk assessment in projects.

The search process in Scopus started on August 17th, 2010 and finished on November 2nd, 2010, while in IEEEExplore and Engineering Village started on November 19th, 2010 and finished on 5th January, 2011.

3.1 Result Analysis

This section presents the result analysis, showing the analysis of selected evidences. To get quantitative data, we performed a data extraction. The following information about all the selected papers was collected:

- Type of environment (see Table 3);
- Whether the paper approaches project risk or operational risk (see Table 5);
- Whether the paper is a conference or a journal paper;
- Information used by the proposed metrics, measures and indicators (see Table 6).

In the classification shown at Table 3, we tried to consider what kind of environment each work explicitly consider. Five types were identified.

<table>
<thead>
<tr>
<th>Type of Environment</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology (IT)</td>
<td>The paper describes metrics or indicators for software development environments and/or any kind of organization that involves information technology services</td>
</tr>
<tr>
<td>Construction</td>
<td>The paper is related to construction environments</td>
</tr>
<tr>
<td>Industrial</td>
<td>The paper approaches risk measurement inside industries or manufacturing</td>
</tr>
<tr>
<td>Research and Development (R &amp; D)</td>
<td>The paper describes environments for research and development projects</td>
</tr>
<tr>
<td>Generic</td>
<td>We consider as generic environment if the paper does not mention for where the proposed metrics or indicators are recommended</td>
</tr>
</tbody>
</table>

Table 3. Types of environments found
Table 4 shows the number of selected papers per environment. We realized that most of the works found is actually related to organizations/environments that explicitly approach information technology.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>15</td>
</tr>
<tr>
<td>Construction</td>
<td>1</td>
</tr>
<tr>
<td>Industrial</td>
<td>1</td>
</tr>
<tr>
<td>R &amp; D</td>
<td>1</td>
</tr>
<tr>
<td>Generic</td>
<td>6</td>
</tr>
</tbody>
</table>

It is important to notice that we defined the search strings for any kind of project environment, and we realize that risk management still is very well accepted at information technology environments in general.

Table 5 presents the quantity of works per type of risk. By Project risk we say that it threatens negatively the success of a project. And by Operational risk we just looked at ones that consider operational aspects of an enterprise, as a whole, especially continuous activities.

<table>
<thead>
<tr>
<th>Type of risk</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project</td>
<td>22</td>
</tr>
<tr>
<td>Operational</td>
<td>2</td>
</tr>
</tbody>
</table>

The indicated result was expected due the fact that the research is focused on project management. Only the references [23, 33] consider operational risks, approaching aspects of organizational changes.

Regarding the type of publication, the number of journals papers was equal to the number of conference papers. This classification is important because works published in journals commonly tend to be more cited because they are commonly more complex, showing not only proposals but also empirical studies.

To get the information and data used by the proposed metrics and indicators to measure risks, we initially listed all information explicitly mentioned in all the selected papers. So, we identified 81 different data and from them we created 11 categories, presented at Table 6.

It is worth mentioning that this categorization allows a better visualization of available information, since metrics and, especially, indicators may have the most varied forms and levels of detail. Thus, we realized that to categorize the information collected is more useful because there were cases where the objective of the measurement was the same, but the entities and attributes used were different.

<table>
<thead>
<tr>
<th>Category of Information</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>The metrics or indicator use information about cost to measure the risks. Commonly, they provide cost monitoring using a risk-driven approach or adapt measurement models from financial risks.</td>
</tr>
<tr>
<td>Time</td>
<td>The metrics or indicators use information about time or schedule to measure the risks. The most of cases aim to make a better control of schedule or time estimation.</td>
</tr>
</tbody>
</table>
Quality
The metrics or indicators uses information about product quality to measure the risks, commonly included at testing activities.

Team
The information used is about the teams characteristics, levels of knowledge, experience, expertise, motivation, turnover, effort rate and levels of communication.

Code
It approaches information about lines of code or another metrics that use the source code as a source of information.

Risk
It uses information directly from each identified risk such as risk exposure (probability of occurrence and impact), number of risks identified and risk dependence.

Size
It approaches information about size of project or size of product, including number of requirements.

Changes
This category just encompasses changes in scope, requirements, implementation or design phases.

Complexity
It is about measures of complexity level of product.

Design
This category approaches metrics or indicators related to product designing process, with focus on the architectural design (for example, reuse rate).

Organizational
It approaches measures directly related to the process or organizational characteristics, such as maturity level (inversely proportional to levels of risk) or any kind of measure of organizational features and security issues.

Figure 2 presents an overview of categories of information collected from the proposed measures, metrics and indicators. It is perceived that there is a slight preponderance of information related to teams characteristics. This fact reinforces that information about projects teams can provide good indicators of risks in multiple project environments, and that views about the skills and capacity of teams should have more weight in measuring the risk level of a project.

![Figure 2. Information category overview](image)

Regarding the Risk category, we found that most of the results use the metric Risk Exposure as a way of risk measurement. Another highlight is the presence of infor-
mation related to Organizational factors, which demonstrates a strong influence of risks in the context of processes. Maturity level usually appeared also at Organizational category, so, it can be an indicator of risk level of an organization, allowing, for example, the decision-making about any kind of investment on an IT organization.

In what follows, we describe and analyze each category of metrics or indicators found.

**Changes:** it comprises changes in scope, requirements, development, and any kind of change could be seen as risk indicators. So, some works affirm that changes could strongly impact in the environment. Kulk and other authors [12] present a set of quantifiable risk drivers for IT environments. One of them considers that aspects of changes in projects, such as in user requirements or changes in scope, proposed by [13] and [14] as well. Regarding changes in requirement, Gupta [15] proposes a metrics called “Mission Critical Requirements Stability Risk Metrics (MCRSRM)”, which assess risk of software product in terms of changes in requirements.

**Code:** some works present source code-based metrics for software risk assessment. Izquierdo-cortazar and other authors [16] and Hosseingholizadeh [17] show proposals that could be helpful in reducing the unused code due turnover and that provide an analysis of the software product to reduce bugs just using information from source code. This kind of information could be helpful when the set of projects use the same programming language.

**Complexity:** only Singaravel and other authors [18] propose a measurement for complexity. Its complexity is related to the product, and this paper only establishes that the complexity of a product is a risk indicator but do not detail the calculation method. On the other hand, it is important to define different indicators considering also the complexity level of a project. If a project is complex, it is somewhat harder to implement because of several types of information, such as project or product size, dependence level, function points, and so on.

**Cost:** the proposed metrics and indicators are specific to financial risks, so that they encompass ideas from Economics. In fact, they are methods proposals of risk assessment given the depth of the functions for calculation aiming to better view chances of return of investment. For example, Pajares and Paredes [19] propose a metric called Cost Control Index, which is used to monitor the cost variance during a project life cycle using Earned Value Management Analysis (EVM). Other methods are: Mean Semideviation Behavior [20] – a method for risk measurement to project selection –, Value at Risk [21] – an existing metric which is combined to help in the balancing of portfolio of engineering and contracting projects –, and Risk Pricing [22] – a specific proposal for software development whose use ideas and insights from financial market to evaluate risks.

**Design:** risk of product design process is highlighted in this category. Customization degree is proposed by [18] and [23]. The former is related to software projects whereas the latter concerns to supply chain. The idea is similar for both works: when the customization degree is high, it is easy the reuse components for production, hence
the efficiency to produce software with good quality is improved. Additionally [23] proposes a risk metric that combines the customization degree and dependence level between product components.

**Organizational:** according to four references [12, 22, 24, 25] the level of maturity of an organization or process is useful to indicate the organizational risk. An empirical study was performed by Wu [25], where shows that some risk factors are reduced when the organizational maturity is high. Some aspects about safety are described in [13].

**Quality:** most of the papers are related to software testing activities. Souza and other authors [26] propose metrics to support the prioritization of test cases based on risk exposure of requirements. They define the number of test cases and change requests as a source of information to measure technical risks, once the test coverage works better when consider risk analysis before testing process. Number of errors is mentioned by Sultan and other authors [27]. This kind of information seems to be relevant specially to address product risks according a database of errors in past similar products.

**Risk:** this category just encompasses found methods and techniques of risk assessment. The Risk Exposure calculation (Probability x Impact) is cited by 5 papers [15, 26, 28, 29, 30]. Wang and other authors [31] suggest the combination between probability of risk factor and concepts of Utility Theory, proposing a function called Utility of Risk Factor, which basically estimate the performance of a project. Number of identified risks is suggested in [26], using this information to visualize risks per class. Another proposal is defined in [32] suggesting the calculation of risk dependence between different projects.

**Size:** two kinds of size were found: project and product. The idea is: when bigger a project/product is, there are more associated risk factors. Regarding project size, Sauer and other authors [33] say that project size is an excellent risk indicator for IT projects, and it made a survey which verify that there is a strong relationship between project size and its performance. About product risk, Kulk and other authors [12] suggest measuring the software, whereas Sultan and other authors [27] suggest number of requirements as a information to product size.

**Team:** even these numbers do not tell us so much about how to define indicators, we can highlight a interesting result: almost a quarter of the raised information consider people as an important aspect to consider during the risk assessment. And it is clearer especially considering software development environment. Perhaps risks factors related to staff must be seen more carefully during the process of risk identification and analysis in projects. Fiedler [34] discusses risk factors related to resistance due to changes in organizations. In this paper some indicators refer to job satisfaction, rate of sick leave and turnover. Turnover is also mentioned in [28] and [16]. There is information about team size [12, 29, 33]. Team skills are mentioned considering experience [12, 35] and knowledge levels [13, 15] on certain technology or platform. There are also proposals of effort estimation based on the team and time to perform, as de-
scribed in [14] and [33]. Motivations levels is considered as an important measure for software development environments [24, 35], once the software processes specifically depends a lot from the staff. And finally, some papers discuss about the importance of communication, so that the communication level must be measured to assure projects or organizational successes [13, 24].

**Time:** the information found about this category is based on project schedule. Pajares and Paredes [19] define a measure called Schedule Control Index, which allow the schedule estimation and monitoring integrated to EVM analysis. A set of indicators is proposed in Turnbaugh [13] and they suggest, but not detail, that it is important to define indicators using the schedule as main source of information.

### 4 Threats to Validity

Despite the correct application of research methods, it is also important to highlight the limitations of this paper so that we can identify points of improvements for future work in this area. In general, we can list the following threats to validity:

- It is based only on three indexing system (Scopus, Engineering Village and IEEE). Although they are useful because it indexes publications from a large number of publishers, the application of empirical research in software engineering is still limited [36], which impacts on the application of systematic reviews and mapping studies;
- The restricted number of years (2004 – 2010) can negatively impact on the results. We just consider these years to consider the state of art of recent works, reflecting the currently overview of the community;
- One single person made the selection of works. It implies that some papers might have been included or excluded incorrectly, even with a clear research question and a protocol built with the authors together;
- The classification of data extracted may have errors because we created it without a tool or statistical method. We just trusted on our experience on the subject to create reasonable categories. Another point is that there were cases where the data in some papers was not so clear to get, so it could skew the results.

### 5 Conclusions and Ongoing Work

Given the diversity of categories found, risk is actually quite abstract, but very present in all organizational levels. Sources of information to assist the definition the metrics and indicators for risk assessment appear in many forms and contexts. Hence, it is necessary to have an appropriate infrastructure to provide the risk assessment on a continuous way, aggregating value to the business and the process adopted. Then, the focus on risks could help to provide a better view of threats and respective opportunities based on real and consolidated data, promoting a risk-driven management.
Considering that this work is a systematic mapping study, it is supposed to find a greater quantity of selected papers in relation to a systematic review. But in this case we can highlight that there is a relatively small number of works in the literature about the process of risk measurement in project environments. In fact, inside IT and software project management there is a gap about this subject. Therefore, the study of risk measurement in software development environments should be seen more carefully, taking into account the aspects of software processes, especially with the increasing of agile methods, which requires a more sophisticated development culture, impacting directly on software processes.

Considering the limitations of this work, discussed at Section 4, it is important as well consider practical applications on the industry to define metrics and indicators. In this light, social aspects must take into account, so that an application of qualitative research methods in order to complement this work may improve the results.

Another challenge is to transform data and information into valuable knowledge, as discussed in [37], which proposes a Risk Breakdown Structure to assist the categorization of risks for IT organizations. Perhaps the usage of information and data to assess risks can make the risk management an activity most often used in software projects environments, by making it less subjective. On the other hand, the selection of information that is necessary for decision-making is not a trivial task, and it requires good skills from project managers to consolidate data into useful and representative indicators.

Finally, it is noteworthy that the presented results are considered as preliminary, since the area of software project management, more specifically risk management, still needs carefully study regarding the use of systematic reviews and mapping studies. Therefore, it is early to consider the results as definitive. Even so, we expect that this work brings initial contributions to the issue of risk measurement in software project management.

This work is an ongoing project. Currently, the whole research has been evolved to define indicators for risk assessment in environments of software projects. The findings from this mapping study were combined with the identification of measurable risk factors from the risk taxonomy of Software Engineering Institute [38], providing, thus, a set of categorized indicators for software development environments. As the main role of an indicator is to support the decision-making process, the definition of indicators may allow a well-founded risk management, supporting managers on the monitoring and analysis of projects just based on information from the environment, providing a better continuous risk assessment.

**Acknowledgements**

We would like to thank FACEPE and CNPq for the financial support given to this work.
References


