Computer-Generated Comprehensive Risk Assessment for IT Project Management

Juliano Araujo Wickboldt, Luís Armando Bianchin,
Roben Castagna Lunardi, Fabrício Girardi Andreis,
Ricardo Luís dos Santos, Bruno Lopes Dalmazo,
Weverton Luís da Costa Cordeiro, Abraham
Lincoln Rabelo de Sousa, Lisandro Zambenedetti
Granville, Luciano Paschoal Gaspary
Institute of Informatics
Federal University of Rio Grande do Sul, Brazil
Email: {jwickboldt, labinchin, rclunardi, fgandreis,
rlsantos, bldalmazo, wlccordeiro, rabelo,
granville, paschoal}@inf.ufrgs.br

Claudio Bartolini
HP Laboratories Palo Alto, USA
Email: claudio.bartolini@hp.com

Abstract—Information Technology (IT) products and services provided by modern organizations are designed in projects that often involve large amount of resources (e.g., humans, hardware, and software). It is essential that organizations enforce rational practices for project management, in order to successfully conclude projects and avoid waste of substantial resources. In this context, Risk Management is fundamental to guarantee the accomplishment of project’s objectives by dealing with adverse and favorable events. Although important, risk assessment in IT projects is usually performed by stakeholders in interviews and brainstorming which may be a very time/resource-consuming task. Therefore, in this paper, we introduce a solution to automate the risk assessment process, based on the history of previously conducted projects. Furthermore, comprehensive and interactive risk reports are proposed in order to ease the analysis of automatically generated reports. The results show that our solution is not only useful to speed the risk assessment process, but also to assist the decision making of project managers by organizing risk information according to the project structure.

I. INTRODUCTION

Many organizations provide services to their customers by means of information technology (IT) infrastructures. The design and deployment of these services are usually made in projects that involve large amount of resources (e.g., hardware, software, and people). Due to the complexity of large IT projects, rational practices for project management should be enforced to ensure that each project will fulfill its requirements avoiding waste of resources. For that end, some libraries and standards on best practices for IT projects have been published, such as the IT Infrastructure Library (ITIL) – proposed by the Office of Government Commerce (OGC) [1] – and the Guide to the Project Management Body of Knowledge (PMBOK) – introduced by the Project Management Institute (PMI) [2].

Every project has risks associated to it, such as exceeding the established schedule or overcoming the initially planned budget. Risks in projects can be faced as events that, if happen, may have positive or negative effects in at least one project objective. These objectives might change according to project’s needs. In this work, we consider a common set of objectives of a project, which are: cost, time, scope, and quality. In order to tackle risk in IT projects, one of the nine so-called knowledge areas from PMBOK is focused specifically on Project Risk Management, whose objectives are: (i) to increase the probability and impact of positive events, and (ii) to decrease the probability and impact of events adverse to the project.

Commonly, in IT projects, the risk assessment process is performed by humans that gather risk information from the stakeholders through meetings, interviews, or brainstormings. Depending on the size of the project, the amount of variables that should be considered for proper risk assessment might turn this process into a very time/resource-consuming task. In addition, the final results may not be as accurate as required, leading project managers to take inappropriate actions to mitigate risks. In this context, risk management must be able to cope with large amount of risk-related variables, and still be intuitive and meaningful for these managers to analyze.

Imprecise and expensive risk assessment based in human knowledge is indeed an issue also in other areas, such as IT change management discussed in ITIL Service Transition book [3]. Recently, some researches have already tackled this problem by automating the risk assessment process [4] [5]. The already proposed methods for automation could be naturally adapted to Project Risk Management. With such an automation, a system would be able to collect information about previous deployed projects and estimate risks for the project under analysis. This would significantly reduce the time spent in gathering information and, moreover, would increase the reliability and accuracy of the results. Still, depending on the project’s size, the resulting amount of information could prevent humans from understanding the risks automatically calculated. We believe, however, that a
complementary solution for summarizing risk information, considering different levels of details, can help project managers to better understand risks in a more interactive fashion.

In this paper we introduce a novel risk information summarization strategy aiming at creating a comprehensive representation of risks in IT projects. Our approach encompasses hierarchically organizing risk information upon different levels of detail, presenting more valuable reports according to the interests of the observer. We assume that IT projects have their risks observed in a hierarchy of six levels: activities, plans, cycles, interactions, releases, and project. In this hierarchy, summarization takes place to combine risk information from one lower level and present it in another more abstract level. Our approach enables project managers to observe risks firstly at a higher level, to then zoom in when they become interested in specific parts of the project.

The remaining of this paper is organized as follows. Section II describes some research efforts that have been carried out to manage risks in IT project management. In Section III we introduce the method for automated risk assessment in IT project management, while in Section IV the strategies proposed for comprehensive risk assessment are detailed. A case study is presented in Section V along with discussions about the results obtained. Finally, the paper is closed with conclusions and future work in Section VI.

II. RELATED WORK

Risk management is subject of research in several different fields. One general purpose standard for organizational risk management is published by the Institute of Risk Management (IRM) [6]. According to this standard, the risk management discipline defines the process whereby organizations methodologically address the risks associated with their activities, aiming to achieve sustained benefits. ITIL encourages the use of a framework for risk management, also proposed by OGC, called Management of Risk (M_o_R) [7]. This framework defines systematic repeatable processes for risk identification and assessment, in a first moment, and subsequent planning and implementation of responses for those identified risks. More focused in the context of IT projects, PMBOK with its Project Risk Management knowledge area, divides risk management into six processes, further detailed in Section III: Risk Management Planning, Risk Identification, Quantitative Risk Analysis, Qualitative Risk Analysis, Risk Response Planning, and Risk Monitoring and Control [2].

Despite the current risk support proposed in the aforementioned frameworks and standards, the adoption of formal procedures in actual projects still demands too much effort, experience, and ability of managers and stakeholders to produce useful results. Kutsch and Hall [8] have investigated the reasons why IT project managers decide whether or not certain identified risks should be considered relevant against project objectives. By interviewing managers from different IT projects, the authors perceived that behavioral factors influence manager’s decisions; therefore the success of risk management is conditioned to their experience. Indeed, when the project manager does not have sufficient experience to effectively prioritize risks, project risk management seems to have little impact on project outcomes, being sometimes even counterproductive. Wyk et al. [9] have evaluated the risk management methods of a large electricity supplier in South Africa. Although the analyzed company employs best practices for risk management, risk identification, analysis, mitigation, monitoring, and reporting are performed employing no automated tool. As a consequence, the company ends up involving an excessive number of stakeholders in risk management process. In addition, there is lack of common practices across various divisions, which turns the reuse of knowledge internally to the company more complex.

In order to aid humans in risk management, the automation of certain steps of the process – such as data gathering for risk assessment – could, for example, potentially reduce the time and cost, while increasing the reliability of results. Probabilistic models are commonly employed in risk management in order to predict undesirable events and also for estimation of metrics, such as cost and time of projects. Fewster and Mendes [10] have proposed a framework, based on a Generalized Linear Model that is capable of estimating probabilities for some project’s negative events (e.g., overcoming project budget or violating deployment deadlines). Bayesian Networks (BNs) have been used in many investigations for similar purposes. Hearty et al. [11] have designed a model, based on BNs, for effort prediction and risk assessment in Extreme Programming (XP) software development projects. Also, Fenton and Neil [12] have applied BNs to predict software defects, while Luu et al. [13] employ it to estimate the likelihood of time-overrun in construction projects. These works have contributed to the automation of risk assessment. However, they concentrate on the prediction of adverse events; the impacts that such events might have over the project objectives are not considered.

Solutions for automation and decision support for risk assessment in IT change management systems have already been proposed in some previous investigations. Based on estimates of time, Sauvé et al. [14] have proposed a risk analysis method to determine priorities for scheduling potentially concurrent Request for Changes (RFCs). Also dealing with scheduling of RFCs, Setzer et al. [15] have modeled the resources of an IT infrastructure as a network of interconnected services; then, risk is quantified by analyzing the impact of changes over affected services.

One particular solution for automation of risk assessment in the planning phase of IT change management, proposed in a previous work of our research group [4] [5], has been used as basis for the contributions in this paper. In that solution, probabilities of failure were estimated analyzing historical execution traces of Change Plans (workflows of activities to perform a change over an IT infrastructure [16]). Besides, the impact of changes was automatically calculated based on the definitions of relevancies of affected elements and their dependencies/relationships. That solution has shown promising results to help on decision making and risk mitigation of changes; hence, it could certainly be adapted to the
context of IT projects. However, the generated risk reports show information about risks of every activity of a Change Plan. Considering that projects might have many activities in their several phases and that risks may affect specific objects of a project, the amount of data in risk reports tend to be too extensive, preventing proper human comprehension. Therefore, in the following sections, we will introduce a novel approach for risk assessment in the context of IT projects.

III. AUTOMATED IT PROJECT RISK ASSESSMENT

In this section we present, in a first moment, the recommendations of the PMBOK for Project Risk Management, emphasizing in which moment automation is needed. Afterwards, a model conceived to represent project management information is detailed, highlighting important classes required to store events that constitute risks. Finally, the solution, adapted from the context of IT change management, to estimate risks in IT projects is presented.

A. Project Risk Management Process

Project Risk Management is a knowledge area that comprises planning, identification, analysis, responses, and monitoring of risks that may affect project objectives. PMBOK divides this process into six processes, as shown in Figure 1 (darker boxes).

![Project Risk Management processes according to PMBOK](image)

Risk Management Planning is the process in which project managers decide how to approach and conduct risk management during the whole project. This process leads to the specification of a Risk Management Plan, which defines of methodology, roles and responsibilities, budgeting, timing, risk categories, and probability/impact matrix for the conduction of risk management in subsequent processes.

Risk Identification is an iterative process that determines the risks that might affect the project and records their characteristics. Among several techniques, risk identification may be carried out by brainstorming, interviewing, or creating checklists based on historical information that has been accumulated from previous similar projects. The output of this process is the initial entries of the Risk Register. The Risk Register is a list of identified risks, potential responses, root causes, and risk categories, which is updated during subsequent risk management processes.

Qualitative Risk Analysis is the process of assigning priorities for treatment of identified risks using their probability of occurrence and corresponding impact on project objectives (such as, cost, time, scope, and quality). Probability and impact are assessed, for each identified risk, in interviews or meetings with project team members or other people from outside the project with extensive knowledge on risk assessment. PMBOK itself recognizes that gathering high-quality information for risk assessment is difficult, and usually consumes time and resource beyond the originally planned.

Quantitative Risk Analysis is the process in which quantitative evaluations are performed for some of the risks prioritized in the previous process. Numerical ratings are estimated for the effects of high priority risks aiming to guide the efforts and intensity of response planning.

Risk Response Planning is the process in which project managers, based on qualitative and quantitative analysis, define options and actions to reduce threats (adverse risks) and enhance opportunities (favorable risks). Response actions should be appropriate to each risk (e.g., in terms of cost). As output of this process, risk-related contractual agreements with other parties (e.g., insurance contracts), as well as recommended changes to the Project Management Plan, may be established.

Risk Monitoring and Control is a continuous process that must be executed during the life cycle of the project in order to keep tracking of the identified risks and detect other newly arising. Occasionally, Preventive Actions (contingency plans) or Corrective Actions (workarounds) planned for risk response result in Change Requests to be handled by the Integrated Change Control (process from outside the Project Risk Management). All approved changes, workarounds, and contingency plans should be documented and attached, in the Develop Project Management Plan process, to the Project Management Plan, which, in turn, should be periodically re-evaluated in terms of risks.

Some problems can be easily identified in PMBOK processes, especially in risk identification and analysis. Firstly, risks are assessed mainly based on human knowledge; hence, the quality of risk management is a function of the experience of stakeholders. The Qualitative Risk Analysis, in addition to consuming too much human resources, may propagate errors to the next processes. Since Quantitative Risk Analysis is optional for low priority risks, some risks wrongly considered as irrelevant may cause damage to project objectives beyond the expectations.

B. IT Project Life Cycle Information Model

In order to enable proper management and reuse of knowledge of IT projects, including management of risk and other
aspects, it is important for organizations to document all activities of developed projects employing a single consistent information model. As far as the authors of this paper are aware of, there is no widely accepted model for representing data of IT projects available in the literature. Therefore, in this work, we propose such a model – depicted in Figure 2 – inspired in a Business Technology Optimization (BTO) software from Hewlett-Packard (HP) called HP Quality Center®.

The participants of activities refer to the ManagedElement class, linking this model with the Common Information Model (CIM) (often used to represent IT infrastructures) from the Distributed Management Task Force (DMTF) [18].

Two classes (bottom of Figure 2) are particularly important for automation of risk assessment: LogRecord and EventRecord. Every Activity performed in a WorkPlan must have an associated LogRecord to it in order to indicate the details of its execution. The execution of an Activity may trigger events (adverse or favorable). These events are documented in instances of the class EventType, along with information about EventType (e.g., adverse or favorable), AffectedObjective (e.g., cost, time, scope, or quality), and Severity (e.g., amount of hours delayed in activity).

C. Automated Risk Assessment Solution

Risk assessment in IT projects is often performed by combining two factors: (i) the probability of occurrence of events (positive or negative) and (ii) the impact that these events might have on the project objectives. A computational system could facilitate this process – usually performed by humans – by calculating both factors using information from a database of previously executed projects. Also, it is important to organize this information in a comprehensive report assisting the managers on decision making concerning to risk mitigation. In a previous work we have proposed a solution for the automation of risk assessment in IT change management area [4] [5]. Hence, in this subsection we briefly explain this solution, emphasizing how it is adapted to the context of IT projects.

Firstly, it is important to keep in mind that risks in IT projects are addressed according to their impacts facing different objectives of the project. Thus, probability and impact have to be assessed separately for as many objectives as managers want to consider. Since the negative side of risks requires more attention of project managers, only adverse events will be considered in the following explanations. However, it is relatively easy to include positive events simply repeating the process.

Intuitively, the probability of occurrence of negative events is calculated per activity in each work plan of a project in four steps:

**First step - Search for executions of similar activities in the database of previously executed work plans:** Since it is a good practice to reuse knowledge in IT projects, activities or even complete work plans might be repeated (sometimes with small modifications) across several projects. Then, in this first step, our solution selects activities that are considered similar to the activity being analyzed. This similarity is calculated by matching the type of activity (e.g., planning, development, analysis, test, or deployment) and its associated participants (e.g., people, computers, or technologies).

**Second step - Calculate Risk Affinity among activities:** Risk Affinity (RA) is a concept introduced in a previous work [5]. Basically, it represents an affinity index, with respect to risks, between two activities from different workflows (the one
contained in the work plan being analyzed and another selected from a project database). It is computed for all activities in both work plans considering their types, participants, and eliminating from the work plans activities that are executed after the pair which the affinity regards to. This elimination has the purpose of removing from the affinity calculation activities that do not affect the activities being analyzed.

**Third step - Count number of executions and events affecting objectives caused by activities:** In this step, our solution investigates, in the LogRecords, the number of executions of each activity selected in the first step and number of events affecting each objective caused by these activities.

**Fourth step - Calculate probabilities of occurrence of adverse events for selected activities weighted by their RA values:** Finally, the probability of occurrence of adverse events is calculated by dividing two values: (i) the sum of occurrences of these events for every selected activity (dividend) and (ii) the sum of executions of the same set of activities (divisor). These values are weighted by the respective RA calculated for each activity.

Impact estimation is calculated following the same steps as proposed for probabilities, except that, instead of counting the number of executions and the occurrence of adverse events (third step), the severity of the event facing the originally planned for the activity is considered. For example, assuming a given activity that was planned to take 8 hours of work to conclude. When it is executed an event is reported informing that it took 4 hours more than it should. The impact that this event represents for the activity’s time objective is the hours that have delayed divided by the hours it was planned to last (in this example impact on time objective is 0.5). The impacts are also weighted using the RA in order to make impact analysis tend to approximate its value to the activities that were executed in more “similar” environments, just as happens to probabilities in step four.

So far, our solution is able to calculate probabilities and impacts of adverse events for every activity in the work plans of a project considering their effects over different objectives. Nevertheless, it is important to display these results in such a way that project managers can actually analyze them. IRM [6] recommends mapping probability and impact values to the following scales: (i) high (more than 25%), medium (between 25% and 2%), and low (less than 2%), for probabilities, and (ii) high (significant), medium (moderate), and low (insignificant), for impact. After that, risks may be classified in one of the nine categories from the matrix presented in Table I. Clearly, the ranges for mapping of probabilities and impacts as low, medium, and high may be adapted to fit the requirements of each project. Also, the risks classification matrix might be extended from 3x3 to a 5x5, for example, to provide more punctual results. These definitions should be made on the Risk Management Plan, before the start of risk assessment.

It is important to notice that, at the end of this classification, each activity of all work plans of the analyzed project will have assigned a risk category facing each different project objective. Depending on the size of the project, it may include a large amount of work plans and, consequently, many activities. To present a risk report to a project manager with hundreds or thousands of lines, taking riskier activities to the top, but possibly losing their context in the project, might not be intuitive enough to help on risk mitigation. The approach then, which is further explained in the following section, is to improve these reports by grouping the risks of activities into higher levels of abstractions (work plans, cycles, iterations, or releases).

### IV. COMPREHENSIVE RISK REPRESENTATION

In previous works, risk reports for IT change management have been typically presented to operators in tabular format, displaying all activities of a certain change ordered by their risk factor. Those reports have shown to be very interesting in pointing risks of failure in activities of change, helping operators to prioritize efforts for risk mitigation by adjusting changes before deployment. Considering that risks in IT projects are analyzed separately for different objectives, a detailed tabular report for any random work plan with five activities could be as shown in Table II.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Cost</th>
<th>Time</th>
<th>Scope</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>1.25</td>
<td>1.00</td>
<td>0.30</td>
<td>0.00</td>
</tr>
<tr>
<td>A2</td>
<td>0.15</td>
<td>0.05</td>
<td>0.05</td>
<td>0.00</td>
</tr>
<tr>
<td>A3</td>
<td>1.15</td>
<td>1.00</td>
<td>0.30</td>
<td>0.00</td>
</tr>
<tr>
<td>A4</td>
<td>0.10</td>
<td>0.00</td>
<td>0.05</td>
<td>0.00</td>
</tr>
</tbody>
</table>

This risk report is not only correct but also provides important information about the risks of all activities of the work plan for as many project objectives as needed. However, large-scale projects might include a huge amount of activities in its several work plans. Thus, for project managers to address the risks of those projects (i.e., composing contingency plans or

---

**TABLE I**

**Risks Classification Matrix**

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Impact</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

---

**TABLE II**

**Tabular Risk Report**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Cost</th>
<th>Time</th>
<th>Scope</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>1.25</td>
<td>1.00</td>
<td>0.30</td>
<td>0.00</td>
</tr>
<tr>
<td>A2</td>
<td>0.15</td>
<td>0.05</td>
<td>0.05</td>
<td>0.00</td>
</tr>
<tr>
<td>A3</td>
<td>1.15</td>
<td>1.00</td>
<td>0.30</td>
<td>0.00</td>
</tr>
<tr>
<td>A4</td>
<td>0.10</td>
<td>0.00</td>
<td>0.05</td>
<td>0.00</td>
</tr>
</tbody>
</table>
workarounds), analyzing one activity at a time could demand too much time and consume excessive resources. Therefore, in this section we introduce a novel strategy to summarize risk reports in different levels of the project (i.e., activities, work plans, phases, interactions, and project). Moreover, risk reports are displayed graphically in two different perspectives: (i) Project Hierarchy View, providing a general project risk overview, and (ii) Work Plan View, displaying more detailed information about risk in specific work plans. Graphical representation of risk reports are further clarified in Section V.

The basic approach of summarizing risk information is to combine a group of values from lower levels of project hierarchy, using a given function, into one single risk metric meaningful for evaluation at a higher level. Furthermore, it is important to keep information apart about the affected objectives in all levels of the project, in such a way that managers can analyze risks over each objective separately. We propose then to use a function to calculate an Average Risk of all risk categories for activities of a work plan, and display this information as the risk metric of the whole work plan. Another important fact is that the result of an average functions tends to smooth all portions into a mean value. For instance, considering that a work plan has four activities, being three of them classified in risk category 9 (lowest possible risk) and only one in category 1 (highest possible risk) for the cost objective. Thus, an arithmetic mean of these values would result in an Average Risk of 7, hiding from the report the damage that one of those activities (classified in category 1) could possibly cause to the project. Therefore, in this work, in order to calculate the Average Risk, we employ a harmonic mean, as shown in Equation 1.

\[
AR = \frac{n}{\sum_{i=1}^{n} \frac{1}{a_i}}
\]  

In Equation 1, \(n\) represents the number of risk values being summarized (e.g., number of activities in a work plan, or number of work plans in a cycle). This number is the dividend of the division by the sum of all reciprocals of risk values (i.e., \(a_i\) is the \(i^{th}\) risk value being summarized). In this equation, we assume that risk categories will always be represented as values ranging from 1 to any greater positive value. Using the aforementioned example (three activities with risk category 9 and one with risk category 1), the resulting Average Risk (\(AR\)) would assign a value of 3 to the hypothetical work plan. The employment of this function works as a pessimistic approach to risk summarization, propagating very high risk activities, detected by the automated solution, up in the project hierarchy.

One final consideration about risk summarization is that Average Risk should always be calculated from risk categories of activities, avoiding the use of other averages computed in higher levels of the project. This is important to prevent the analysis from losing information about the cardinality of summarized sets (e.g., number of activities in work plans, or number of iterations in a release). For example, considering a given cycle with two work plans, one containing 20 activities and another with only 2. Once Average Risks are calculated for both work plans, these values will belong to the same range (i.e., from 1 to 9 continuously), and no information is kept about work plans amount of activities. If an Average Risk for the cycle is calculated considering the computed average from its two work plans, some risky activities from the largest plan could be attenuated. To tackle this problem, there are two options: (i) to calculate the Average Risk of the cycle from all 22 activities from both work plans, or (ii) to use a weighted harmonic mean of the Average Risks from work plans, where the weights are their cardinals (respectively 20 and 2). Both options produce exactly the same results, although the second is better to avoid recalculation of average values up in the hierarchy of the project.

V. CASE STUDY

Aiming to prove concept and technical feasibility of the proposed solution, we have conducted a case study considering a hypothetical software development project. Also, a database was designed containing synthetic information about work plans from other projects, execution of activities, and documented adverse events. In this section, in a first moment, we briefly present the hypothetical project’s structure. Afterwards, comprehensive risk reports automatically generated by the solution are shown under two different perspectives: Project Hierarchy View and Work Plan View.

A. Hypothetical Project Structure

The goal of the studied project is to develop a system for monitoring, supervision, incident reporting, and problem diagnosis on large-scale corporative networks. The purpose of this system is to provide a company with support for management of an IT infrastructure inventory, monitoring, and supervision of Configuration Items (CIs) (e.g., routers, computers, software packages, and services), and also record incidents involving these CIs, assisting the problem diagnosis process. According to high level definitions of requirements for the project, a project manager split development efforts into four releases, as follows:

- **Release 1**: Monitoring and supervision basic features;
  - **Iteration 1**: Database modeling to allow composition of IT infrastructure inventory;
  - **Iteration 2**: Development of server-side core module application;
  - **Iteration 3**: Development of client-side core module application;
  - **Iteration 4**: Development of server-side graphical Web interface basic operations;

- **Release 2**: Monitoring and supervision advanced features;
  - **Iteration 1**: Development of server-side advanced reports composer;
  - **Iteration 2**: Development of server-side analytical multivariable graphics module;

- **Release 3**: Monitoring and supervision integration;
- **Iteration 1**: Development of server-side SNMP support module;
- **Iteration 2**: Development of server-side Web Services support module;
- **Release 4**: Incident reporting and problem diagnosis;
- **Iteration 1**: Database modeling for incident reporting;
- **Iteration 2**: Development of incident reporting Web interface;
- **Iteration 3**: Development of problem diagnosis tool.

In Release 1, basic functionalities of the system are implemented. In its first iteration, the database to allow representation of CIs from the IT infrastructure is modeled. The core of the system works as a client-server application, where the server requests/receives information about managed clients installed in CIs. The Web interface basic features are also delivered in first release, such as CRUD (Create, Request, Update, and Delete) operations over registered objects. Advanced features, such as reports composition (e.g., availability, network load and latency, and alarms) and graphs for data visualization, are left to the second release. In the third release, modules for integration with SNMP and Web Services are included to enable management of devices that support those management interfaces. Finally, in the fourth release, incident reporting interface and a diagnosis tool are added in order to allow association of reported incidents and problems with corresponding defective CIs. Although not detailed above (due to space limitation), every iteration of the project is divided into four cycles: Analysis, Project, Development, and Testing.

### B. Comprehensive Risk Reports

The project analyzed in this case study contains 141 activities disposed in 34 work plans. Since the automated risk assessment solution calculates four risk categories (one for each affected objective) for all activities of the project, a risk report as shown in Table II could not be practical to help on decision making for risk response planning. Instead, the new approach proposed in this paper generates more comprehensive reports under two perspectives: (i) Project Hierarchy View (Figure 3-a), which gives an interactive overview of risks using the project hierarchical structure, and (ii) Work Plan View (Figure 3-b), useful to investigate particularly risky work plans aiming to understand the sources of risk.

As shown in Figure 3-a, a project manager can interactively choose which part of the project he/she wants to inspect with more details. For example, by expanding (+) an iteration the risks calculated for all of its cycles are displayed. Analyzing this hierarchical report one could notice that, among all releases, the first one holds most of the risks from the hypothetical project analyzed in this case study. Inspecting Release 1, a project manager may figure out that Interaction 4 requires special attention due to its risk factors in all objectives. Observing the cycles of Interaction 4, it is possible to notice that risks of different objectives are mostly distributed among Cycles 1, 3, and 4. Cost and Scope risks are negatively influenced by Cycle 3, Time risks are shared between Cycles 3 and 4, and Quality risks are more evidenced in Cycle 1. A report with these characteristics indicates that, in past similar projects automatically analyzed by our solution, events were reported evidencing poor quality in activities of analysis. That might have caused other adverse events to happen affecting cost and time of later development and testing cycles.

Whenever a project manager needs to inspect with more details some of the work plans from the project, the Work Plan View may be used. In Figure 3-b, one work plan from Cycle 3 (Development) of the fourth iteration from the hypothetical project is shown. The detailed work plan defines six development activities necessary to implement basic functionalities of the Web interface of earlier described system. Initially, administration of credentials (e.g., login forms, users names, passwords, and access rights) and system menu structure (e.g., sections and subsections) are developed. In a subsequent moment, two parallel branches are started. Both branches develop DAOs (Data Access Objects), for persistence of objects in a relational database, and development of Web forms for CRUD operations of CIs and their categories. The risk classifications automatically assigned to the activities are displayed next to each of them in the work plan structure. This visualization helps the identification of problematic activities that might compromise the success of the work plan.

One important fact is that, despite the attenuation caused by the summarization of risk classifications, automatically calculated risks of activities still reflect very well in upper levels of the project. This is clearly visible in the hierarchical view (Figure 3-a) used as example in this case study. Some activities from different cycles in Interaction 4 had high risk rating (low categories) and this reflected in high risks for the whole Release 1. Based in these reports a project manager could prioritize risks and establish directions for risk response. For example, one strategy could be addressing risks of a project by iteration. Then, a threshold may be specified defining that preventive actions (contingency plans) are required for iterations with risk factors below 5, and corrective actions (workarounds) for iterations that exceed this value.

### VI. CONCLUSION & FUTURE WORK

In this work, the need for rational IT project management have been discussed, emphasizing how it is supposed to help organizations to conduct successful projects saving substantial resources. In this context, risk management plays a key role in the successful accomplishment of project objectives. Nevertheless, we have argued that current risk assessment practices, in addition to consuming too much human resources/time of the project, still do not present clear results in practice. Thus, in this paper, we have introduced a solution to automate the risk assessment process in IT projects by investigating the database of events documented in past projects. Also, more comprehensive and interactive reports have been designed to aid the decision making on risk response planning.

The automated solution proposed has shown to be useful to speed the process of risk assessment, since it is based on information retrieved from a database of previously executed
projects and does not require any human intervention. Remarkably, the reports generated organize information according to the project hierarchical structure, facilitating the identification of risks in each phase of the project. The proposed risk information summarization strategy achieved its objective, which was to combine risk information from activities of work plans displaying this information into higher levels of the project without hiding risks from lower level.

In future work, we intent to use data from real life projects to better evaluate the applicability of the proposed solution. Also, it would be interesting to conduct a survey and receive feedback from experienced project managers and stakeholders to evaluate the usability of the proposed risk reports.

ACKNOWLEDGMENT

This result was achieved in cooperation with Hewlett-Packard Brasil Ltda. using incentives of Brazilian Informatics Law (Law nº 8.248 of 1991).

REFERENCES