GAIA Risks: A risk management framework

F. H. Gaffo
Department of Computing
State University of Londrina
Londrina, Brazil

R. M. de Barros
Department of Computing
State University of Londrina
Londrina, Brazil

Abstract

Nowadays, organizations face a lot of challenges due to the volatility of the scope and requirements that software may contain. This change leads to problems that directly affect the quality of the final product. In order to avoid these problems, even in early stages of the project, the software development process must be able to handle risk management. In this context, it is easy to find some ready-to-use models. However, methodologies that quantitatively assess the software development process and point to actions for its improvement, recording the progress of the activities through metrics, were not found. This paper presents a service-based risk management framework which comprises five maturity levels, a deployment process, a diagnostic assessment questionnaire and relevant metrics to the process, which should be stored in a historical database to serve as a basis for future estimates.

Keywords: risk, risk management, software engineering, project management, metrics

1 Introduction

Information systems are widespread in many sectors of modern life, being present from hospitals to leisure activities, and people are increasingly dependent on them in their daily activities [1]. However, companies that develop those systems, face a number of challenges such as cost reduction, deadlines meeting, specification errors and low quality of the product.

Those above-mentioned facts can be proven by the Chaos Manifesto [2], which indicates that, although the percentage of successful projects has increased over 2010, only 37% of them are delivered on time, with planned costs and meeting the stipulated requirements, other 42% suffer from delays, high costs or specification problems, while the 21% remaining are cancelled.

Risks can be seen as the effect of the uncertainty on project objectives that result in impacts (positives or negatives) on businesses. The Risk Management (RM) process comprises a set of coordinated activities to direct and control an organization with regard to risk. The Risk Management Framework is a set of components that provide arrangements to design, implement, monitor, review, and continually improve of RM [3].

Thus, the aim of this paper is to present a framework, named GAIA Risks, whose purpose is to provide a flexible structure to manage risks inside a software development organization. The designed framework is basically comprised of: (1) five maturity levels; (2) seven services; (3) one assessment questionnaire; (4) four reassessment checklists; (5) RM performance indicators and also (6) a historical database of RM metrics.

The development of this framework is carried out through the fragmentation of the ISO 31000 RM process in seven services, which aims to deliver value to the consumers, helping them reach their goals [4]. Each service, in its turn, organizes: (a) documents templates; (b) tools and techniques; (c) vocabularies; (d) workflows, and also (e) performance indicators.

The metrics obtained through the performance indicators of the GAIA Risks Framework are stored in order to create an RM organizational memory. This record represents the evolution of this management within the software development process. The performance indicators will be better presented in section 3.

This paper is organized as follows: section 2 shows some RM related works found in literature; section 3 exposes the GAIA Risks, its services and other components; section 4 covers GAIA Risks implementation study case. Finally, in section 5, conclusions, contributions and future works will be addressed.

2 Literature Review

Several studies have been done in the risk identification, analysis and assessment areas, in general, about the management process, which Boehm [5] is one of the pioneers, purposing a spiral model to man-

age risks. Currently, there are several methodologies to manage project risks, among which the most important are the process and framework based models [6]. This section comprises a review of some RM related work found in literature and also some widely used approaches.

2.1 Related Work

Several methodologies to manage project risks are found in the literature, among which are present approaches that are based on the development of an institutional memory to assist the stakeholders in all stages of management [7, 8, 9]. In those studies, the presence of a risk information repository is common, this institutional memory contains trivial and relevant data about them, which helps in the decision making process.

In other cases, it is necessary to manage risks in distributed software development environment. Leme [10] proposes a set of procedures specially designed to identify, analyze, evaluate and treat risks in this scenario, in order to disseminate information obtained and learned lessons in all development sites. Another aspect addressed by this study is the RM learning process, for this, the author presents a tool to assist the operations.

However, in internationally distributed projects, it is necessary to spread the information in a rapid and effective way among all development sites. Some authors show a model that uses the internet to perform such activities [11, 12, 13], proposing the creation of a risk database, with their causes, consequences, metrics and the realized treatment, in order to assist the decision making process and facilitate the data dissemination in all development sites.

Another model for managing project risks is the process used by the agile methodologies, such as SCRUM [14] and Extreme Programming (XP) [15], where the management is performed iteratively and incrementally, inside the sprints, which are held over a period of a month or less, when a usable version of the product is created. Among the main objectives of these meetings, one is to improve predictability of risks and manage them effectively through empirical techniques.

In turn, some authors present the RM through modeling and simulation [16, 17], whose realization is given by an experimental design that aims to help managers understand the environment, test, analyze the obtained data, help to determine the best treatment option and identify the rise of new risks.

We also found works that address the RM collaboratively and concurrently among the projects of an organization [18, 19]. Both studies show processes that predict the emergence of arising risks from the relationship between the projects maintained by a company. However, the study made by Wanqing and Yong allows, in addition to other features, to shape this management within the needs of each project, the costs and investments.

Recently, several studies have been done to manage the risks of outsourcing software development [20, 21, 22]. In these studies, the authors assert that the risks of outsourcing are still little explored, but propose models and frameworks to identify, analyze, assess, treat and monitor risks.

Among the researched papers, one resembles the proposal of this paper and presents a maturity model for the RM process, which allows assessing, classifying and analyzing processes according to the standards of CMMI [23]. However, the implementation process or the ability to customize the proposal are not addressed. Also, the process is not service-based.

Finally, the RM process of some widely used approaches, which are based on processes and activities of identifying, analyzing, evaluating, treating, communicating and monitoring risks, were researched [24, 3, 25]. The main objective of these models is to predict the problems in order to reduce the chance of failure, avoiding the reworking costs or occurrence of unidentified risks.

3 Framework to Manage Risks Through Services

As shown before, the aim of this paper is to present a framework, named GAIA Risks, which is service-based and focuses on helping project managers to include RM practices on a Software Development Process (SDP), without the need of major changes neither on the SDP nor on the organizational structure of the business.

This set of services has as main goal deliver value to customers helping them to achieve their objectives. Among its main features it stands the ability to group and arrange, in a single web-based environment, tools, techniques, documents templates, workflows and vocabularies that are common to the each RM step. Another important feature of this framework is the RM customization for each need of the project, customer or organization.

Thus, to obtain the services that make up the GAIA Risks Framework, the management process proposed by the ISO 31000 standard was broken into seven services: (1) Identification; (2) Analysis; (3) Evaluation; (4) Treatment; (5) Context Establishment, (6) Monitoring and review, and also (7) Communication and Consultation. The organization of the

service on maturity levels follows the MMGRSeg criteria, which has well established rules for each maturity level, as shown in Figure 1.

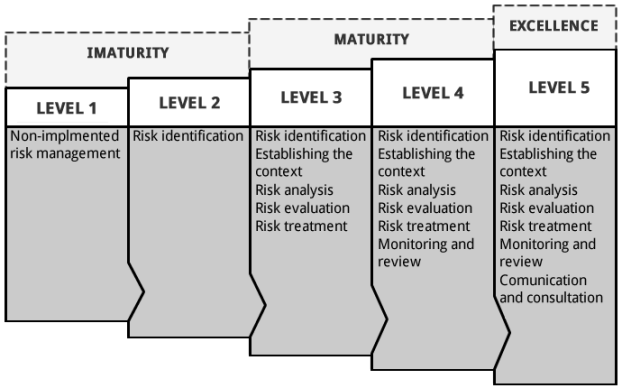

Figure 1: GAIA Risks Framework.

The model consists of five maturity levels sorted into three stages: (1) immaturity, (2) maturity, (3) excellence, as illustrated on Figure 1. Although the MMGRSeg [26] model has a focus on information security, its criteria are perfectly applicable to the software development, due to the fact that they were based on the CMMI model.

Each GAIA Risks maturity level comprises services. Each service has five knowledge areas, which are responsible for maintaining the information organized and can be customized according to the needs of each organization. The Figure 2 shows a graphical representation of the service structure.

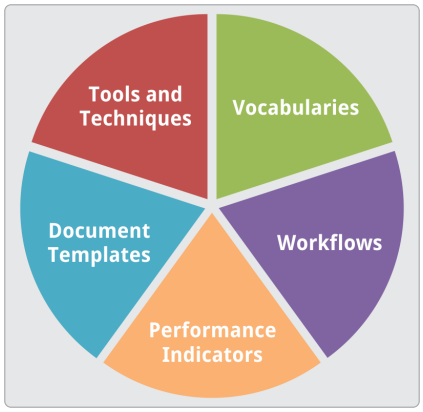

Figure 2: GAIA Risk Service Structure.

As presented in Figure 2, the basic information that composes the service areas are obtained from different standards, such as: (a) the tools and techniques come from the ISO 31010 [27]; (b) the document templates are taken from the PMBOK [24] guide; (c) the workflows are based on the ISO 31000 standard; and also (d) the vocabularies are taken from ISO Guide 73 [28].

However, as the goal of GAIA Risks is to offer a flexible structure that fits both the needs of the client, team and product, the information present in each of the service areas can be customized according to the needs and possibilities of each organization. This personalization is not described by other authors.

GAIA Risks is available in a web environment that is accessible throughout the organization on a fixed address (`http://www.gaia.uel.br/gaia_riscos`), ensuring that all team members have access to the knowledge offered by the structure, its services and peculiarities.

Finally, to implement GAIA Risks in its SDP, the organization must comply with an implementation process, checking every level evolution, in order to ensure that changes are consistent with the framework structure and fully meet their expectations.

3.1 GAIA Risk Deployment Process

In order to apply the GAIA Risks Framework to a SDP, a set of activities, named GAIA Risks Deployment Process (GRDP), are developed. This process involves activities that must be followed. Those actions intend to indicate the maturity level of the SPD, re-evaluate the adherence of the process to a maturity level, measure the ability to evolve to the next level and record the performance indicators. The GRPD activities are illustrated in Figure 3.

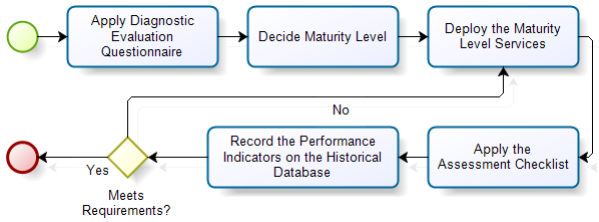

Figure 3: GAIA Risks Deployment Process.

As shown in Figure 3, the entry of all deployment process is the completion of a Diagnostic Assessment Questionnaire (DAQ), which must be answered electronically through the Diagnostic Assessment System (DAS). In turn, as a result of this questionnaire, we are able to obtain the positioning of the SDP in one of the five maturity levels of GAIA Risks Framework.

This position is presented to the user of the system through a radar chart whose axes represent the services. The percentages in each axis represent the maturity level. The lower percentage obtained on the axes determines the maturity level of the process. The scale to transform percentage into maturity level is:

- **0% to 20%:** Level 1 of Maturity.
- **21% to 40%:** Level 2 of Maturity.
- **41% to 60%:** Level 3 of Maturity.
- **61% to 80%:** Level 4 of Maturity.
- **81% to 100%:** Level 5 of Maturity.

The DAS makes it possible to manage and answer questionnaires. In the administrative area it is possible to control users, questionnaires, chart axes, issues and alternatives. In the common area the visitor can register themselves. Once registered, the user can answer questionnaires and manage their responses. The results are reports that will guide the deployment of the GAIA Risks on the organization SDP.

Through the answers, DAS presents, as part of the results, the necessary improvements to be made in the SDP, taking into account the achieved maturity level. This process seeks to ensure continuous RM improvement, done through evaluation checklists, indicating the compliance of the process with the achieved maturity level.

Other products of great importance, obtained at the end of the GRDP, are the Performance Indicators, which must be stored in organization's historical database after completing the evaluation checklist. The purpose of these metrics is to create an RM memory and provide a basis for future estimates. Table 1 describes the key metrics obtained during the implementation of the GRDP.

Table 1: GRDP Metrics Summary

Metric	**Description**
Identified Risks	Record the amount of risks that have been identified..
Treated/Mitigated Risks	Record the amount of risks that were treated or mitigated..
Accepted/Transferred Risks	Record the amount of risks that were accepted or transferred.
Risks That Occurred	Record the amount of risks that occurred.
Generated Rework	Record the amount of generated rework.

Each metric shown on Table 1 is, in turn, decomposed into purposes of measurement, calculation formula, unit of measure, responsible for the measurement, measurement frequency and other information, following the Balanced Scorecard methodology [29]. Table 2 exemplifies the metric that measure the total amount of identified risks.

Table 2: Total Risk Identified by Use Case Points

Identifier	TIR.
Name	Total of Identified Risks.
Measurement Objective	Track the absolute number of identified risks.
Purpose of the Associated Business	Identify the maximum number of the risks.
Formula	TIR = Total of Identified Risks.
Measurement Interpretation	As more risks identified less chance of surprises.
Responsible for Measurement	Project Manager.
Frequency of Measurement	Will be held after the application of the checklist.
Data Source	List of Identified Risks.
Unity	Integer.
Goal	Identify the highest number of risks.
Target	All stakeholders.
Frequency of Analysis	Whenever there is a measurement of the total number of identified risks.
Responsible for Analysis	Project Manager.
Analysis Method	After measurement.

Finally, when all entries of the evaluation checklist are not met, it is necessary to make changes to include the remaining services, or specific areas that have not met the checklist requirements. At the end of the GRDP, with the achievement of all objectives of the checklist, it becomes possible to evolve for the next maturity level and execute the GRDP again.

4 Implementation of GAIA Risks on a Software Development Process

In order to verify and validate the framework for managing project risks through services (section 3), the deployment process (section 3.1) was executed iteratively until the GAIA Factory Software Development Process (GFSDP) reach the RM excellence (maturity level 5). With this purpose, two projects of GAIA Factory[1] were used. Table 3 shows a summary of the

[1]The GAIA Software Factory consists of teams of students from undergraduate and master's courses from the Department of Computing (DC) of the State University of Londrina (UEL) and uses a prescriptive development process, designed gradually to meet the level F of the MPS.Br [30], in order to standardize the processes, increase the quality of produced software, the customer satisfaction and the staff productivity.

changes made in the GAIA Software Development Process.

Table 3: Summary of GFSDP Changes

Modified Activity	**Type of Change**	**Referred Services**
Initial Analysis	Work Instruction	Establishing Context
Analysis and Planning	Activity Inclusion	Risk Identification, Analysis and Evaluation
Execution and Implementation	Activity Inclusion	Risk Treatment
Delivery	Activity Inclusion	Monitoring and Review
Manage Communication	Work Instruction	Communication and Consultation

5 Conclusions

The RM is an increasingly trivial factor to project success, once the current market volatility, the ever-changing requirements and scope may create obstacles to reach success or reduce the quality of the end product. Thus, this paper shows a service-based framework, named GAIA Risks, which also has five maturity levels and whose objective is to manage the inherent project risks with flexibility.

According to the presented paper it is possible to conclude that the structure created (section 3) organizes, through the services, the best knowledge of the RM standards and methodologies, allowing its customization, tailoring the activities to the needs of the team, project and client simultaneously.

The possibility of integrating RM to an organization SDP through PDCA cycle, in conjunction with the maturity levels, as shown in section 3.1, makes it possible to implement it total or partially, allowing it to evolve over time, until excellence. The structure becomes broad and can be used in designs that require a greater or lesser risk treatment.

Another relevant aspect of the GAIA Risk is the possibility of measuring the efficiency of RM within an SDP and also the possibility of comparing the results with the indices obtained in other processes of the organization. Furthermore, it becomes possible to use these metrics in other managements, such as human resources management.

Future works are related to the subject: (a) increase the number of case studies aiming to improve the GAIA Risks Framework, applying it to other areas such as governance and other industry branches, (b) develop an automated tool to support RM, in which the learned lessons aids the project managers to determine the services that best fit their needs and (c) create a tool to manage metrics.

Finally, after this study, the main contributions were obtained: (a) establishing a framework for managing risks through services, whose structure has five levels of maturity (section 3); (b) seven services that are composed by the best practices of widely used standards (section 3); (c) a deployment process for RM (section 3.1); (d) a Diagnostic Assessment System that positions the software development process in one of the maturity levels (section 3.1); (e) indicators to measure the RM performance (section 3.1); and also (f) checklists to guide the deployment of services (section 3.1).

References

[1] S. Islam and W. Dong, "Human Factors in Software Security Risk Management," *Risk Analysis*, pp. 13–16, 2008.

[2] Standish Group, *Chaos Manifesto*, 2011.

[3] ISO, *ISO 31000: Principles and Guidelines*, 2009.

[4] ITSMF, *An Introductory Overview of ITIL ® V3*, A. Cartlidge and M. Lillycrop, Eds. The UK Chapter of itSMF, 2007.

[5] B. Boehm, "Software risk management: principles and practices," *Software, IEEE*, no. January, 1991.

[6] P. L. Bannerman, "Risk and risk management in software projects: A reassessment," *Journal of Systems and Software*, vol. 81, no. 12, pp. 2118–2133, Dec. 2008.

[7] R. Riehle, "Institutional memory and risk management," *ACM SIGSOFT Software Engineering Notes*, vol. 32, no. 6, p. 5, Nov. 2007.

[8] S. Alhawari, L. Karadsheh, and A. N. Talet, "Knowledge-Based Risk Management framework for Information Technology project," *Information Management*, p. 16, 2011.

[9] U. Rosselet and M. Wentland, "Knowledge management framework for IT project portfolio risk management," *Fifth International Conference on Knowledge*, pp. 203–204, 2009.

[10] L. H. R. Leme, "Uma estratégia para apoiar o gerenciamento de riscos em um ambiente distribuído de desenvolvimento de software," Master's thesis, Universidade Estadual de Maringá, 2007.

[11] S. H. Han, D. Y. Kim, and H. Kim, "A web-based integrated system for international project risk management," *Automation in construction*, pp. 342 – 356, 2008.

[12] A. A. Keshlaf and S. Riddle, "Risk Management for Web and Distributed Software Development Projects," *Fifth International Conference on Internet Monitoring and Protection*, pp. 22–28, 2010.

[13] A. Lamersdorf, J. Munch, A. F.-d. V. Torre, and C. R. S´nchez, "A Risk-Driven Model for Work Allocation in Global Software Development Projects," *IEEE Sixth International Conference on Global Software Engineering*, pp. 15–24, Aug. 2011.

[14] K. Schwaber and J. Sutherland, *The Definitive Guide to Scrum: The Rules of the Game*, 2011.

[15] H. Mathkour, G. Assassa, and A. Baihan, "A Risk Management Tool for Extreme Programming," *International Journal of Computer Science and Network Security*, vol. 8, no. 8, pp. 326–333, 2008.

[16] U. Chinbat and S. Takakuwa, "Using Simulation Analysis for Mining Project Risk Management," in *Proceedings of the 2009 Winter Simulation Conference*, 2009, pp. 2612–2623.

[17] D. Liu, Q. Wang, and J. Xiao, "The role of software process simulation modeling in software risk management: A systematic review," *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pp. 302–311, Oct. 2009.

[18] C. Gusmão, "Um Modelo de Processo de Gestão de Riscos para Ambientes de Múltiplos Projetos de Desenvolvimento de Software," Master's Thesis, Universidade Federal de Pernambuco, 2007.

[19] L. Wanqing and Z. Yong, "Study on Risk Management System for Construction Enterprises Based on Projects," *4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–5, Oct. 2008.

[20] D. Schreiber, C. d. S. Garcia, and D. Domingos, "Terceirização de Desenvolvimento de Software em Body Shop: Uma Proposta para Diminuir os Riscos," *X Simpósio Brasileiro de Qualidade de Software*, p. 8, 2010.

[21] X. Shi, H. Tsuji, and S. Zhang, "Eliciting experts' perceived risk of software offshore outsourcing incorporating individual heterogeneity," *Expert Systems with Applications*, vol. 38, no. 3, pp. 2283–2291, Mar. 2011.

[22] L. M. Abdullah and J. M. Verner, "Analysis and application of an outsourcing risk framework," *Journal of Systems and Software*, p. 23, Feb. 2012.

[23] M. Aldenucci, "Um modelo de maturidade para processos de gerenciamento de riscos em projetos," Master's Thesis, Pontifícia Universidade Católica, 2009.

[24] PMI, *A guide to the project management body of knowledge*, 4th ed. Newton Square, Pennsylvania: Project Management Institute, Inc., 2008.

[25] F. Turley, *The PRINCE2 Training Manual: A common sense approach to learning and understanding PRINCE2*, 2010.

[26] J. Mayer and L. L. Fagundes, "A model to assess the maturity level of the Risk Management process in information security," *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops*, no. 5, pp. 61–70, Jun. 2009.

[27] ISO, *ISO 31010: Risk Assessment Techniques*, 2009.

[28] ——, *ISO Guide 73: Risk Management Vocabulary*, 2009.

[29] R. Kaplan, D. Norton *et al.*, "The balanced scorecard–measures that drive performance," *Harvard business review*, vol. 70, no. 1, pp. 71–79, 1992.

[30] SOFTEX, *MPS . BR - Melhoria de Processo do Software Brasileiro Guia Geral*. Brasília: Associação para Promoção da Excelência do Software Brasileiro, 2011.