Security Risk Management in IT Projects based on Workflow Mining

Nkondock M.B. Nicolas
University of Yaounde I
Department of
Computer Science

Etame M. Frankie
University of Yaounde I
Department of
Computer Science

Atsa E. Roger
University of Yaounde I
Department of
Computer Science

ABSTRACT

Over time, IT projects face several risk that can lead to failures, like security ones. Thus, security risk management and risk management in general in a project is a major issue that the success of the project depends. The sources of security risk are varied in an IT project. Risks should be a comprehensive study by the IT project managers in order to prevent or stop their harmful effects. In this paper, a new approach based on the workflow mining and to manage security risks in an IT project is defined. It is based on the analysis of event logs associated to resources used in a project to identify and analyze security risks therein and therefore able to offer a solution to address them. As a result, patterns of identification and treatment of risks are proposed on the basis of a policy of risk management.

Keywords

Risk, risk management, IT project, workflow mining

1. INTRODUCTION

Nowadays, most companies computerize their information systems; The aim is to automate various processes therein. Thus, many IT projects are emerging but still do not reach their destination due to their mismanagement. When risk are not properly controlled, it can derail projects. Yet it is not uncommon to see projects through to serious and costly failures (both from a technical point of view, a financial or commercial), a degradation or questioning of their main objectives (cost, time and quality), or their outright abandonment. The study "CHAOS - 2013" of Standish Goup [1] shows that generally was 16.2% success rate, 52.7% over budget or late and 31.1% drop for a total of 83.8% failures. Faced with such a situation, it becomes necessary, indeed imperative, for those conducting various projects (managers, project managers, business managers, members of project teams ...), to better understand the potential risks associated with their project, to reflect on how to anticipate, analyze and control them better. In Cameroon the government commitment is to build an emerging country by 2035, the achievement of this objective requires the realization of major projects, which indicates the major issue of fluency and organization technical environment in which to implement projects and a perfect management of risks associated with them, hence the great importance of this study, axed on security risk.

Risk management is divided into 5 main stages, namely [2]: planning of risk management, risk identification, risk analysis, planning risk responses and finally monitoring and risk control. The planning phase of risk management appears to be of paramount importance because outputs the risk management plan (RMP) is the compass in the assessment, treatment, monitoring and risk management. Terms of risk management is even more important that consists of a basic element: risk response plan. It identifies the risks that may occur during the project and everyone associated with adequate treatment. Writing the plan risk response is naturally a challenge for risk management. Specifically, the current challenge is how to build the list of risks from an old project and can be used for risk assessment in future projects. [3]

Faced with the objective mentioned above, a risk management approach based on the workflow mining [4] to ensure the achievement of the objectives of a project is defined. The remainder of this paper is organized as follows: Section 2 provides a review of the literature on risk management and workflow mining, Section 3 presents the scientific concepts needed for this model, Section 4 presents the proposed method for risk management, section 5 concludes this work and presents different perspectives and future work.

2. STATE OF THE ART

This section presents a review of the literature in our various fields of study.

2.1 Risk management in IT projects

The risk [5]" is the effect of uncertainty on objectives." The risk is defined in [6]" as a measurable uncertainty" to mark the distinction between risk and uncertainty is immeasurable. Furthermore, the risk [7] is an uncertain event (or condition), if it occurs (if it is satisfied), has a positive or negative effect on project objectives particularly on time, cost, and quality. A risk may have one or more sources whose occurrence may have one or more impacts on the project. A literature review of more than a thousand Canadian organizations shows that the main reasons for failure of IT projects are inadequate risk management and poor project planning. [7] Risk management is a particular discipline that integrates knowledge from many other disciplines.

The generic definition of risk management [8] is the appreciation and reduce potential risks from their source or origin. Risk management [7] deals identify risks, understand, and develop a plan for responding to risks to minimize their effects.

The process of risk management is described in six steps [9]:

1. **The definition of objectives:** review of the initial objectives of the project, refinement and description implicit objectives and constraints explicitly;
2. **Identification:** identification of potential project risks using various approaches;
3. **Analysis:** classifying risks, complete their scenarios, assess their effects, their likelihood estimate;
4. **Planning and Control:** select the most important risks, propose control actions;

5. **Control:** Implement control actions;
6. **Monitoring:** Monitorer risk situations

In General, The process of risk management involves the following main steps:

1. Risk identification
2. Risk Analysis,
3. Planning risk,
4. Monitoring risk.

2.2 Workflow mining

The goal of workflow mining is to extract information about processes thanks to event logs analysis. Every log considered contents events linked to a specific resource used in a workflow execution. The life cycle of workflow contains 4 phases: (1) The workflow conception that helps to build a model based on information to identify

The life cycle of a workflow is divided into four phases [23]: (1) Workflow Design (design phase) that allows the development of a model based on timely information and whose objective is to identify the different activities and constraints; (2) Workflow Configuration (the configuration phase) on the limitations and characteristics of workflow management system, taking into account certain objectives of the organization; (3) Workflow Enactment (the integration phase) which deals with the integration of new features in Workflow System under the new terms based on the strategy of the organization. In this phase the information system is aligned with the vision of the organization. And (4) Workflow Diagnosis (Phase diagnostic or evaluation), where data from the Workflow instances are analyzed. This analysis may lead to a new workflow or new elements for the design of a new Workflow, completing the life cycle of the old. Workflow Mining can therefore be important in risk management because it allows the development of what is actually done by constructing the corresponding to the actual situation or system status information in terms of execution of model activities (Workflow). The model is constructed on the basis of information obtained from the phase of implementation. Related data are stored in the logs of the information system. These logs keep track of all the events taking place there for future analysis that precede a decision. The workflow mining compares what actually happened to what has been previously defined. Monitor the activities taking place at runtime can also detect the differences between the model built in the analysis phase of the project and the actual activities recorded in the project. The use of workflow minning in this work is to show how models are designed workflow from the Workflow Event Logs (event log), but to make the identification of risks and their salaries from Event Logs while relying on the model of the project defined in the analysis phase of it.

2.3 Related work

In the literature, several approaches exist to identify and / or assess the risks [24, 25, 3. 26]. Wickboldt and al. [26] proposed a framework that uses data from the execution of processes for risk assessment. This framework uses the information risk activities already carried out in the project. Difficult to perceive a risk not yet appeared is a weakness of this approach. Jallow and al. [25] proposed a framework for identifying the risks of operational processes. However, the assessment of probabilities, the impacts associated with activities, risk derivatives is made by experts. It is best to avoid subjective opinions and observe such values of historical data for similar projects. Shareeful Islam [3] proposes a model for risk management based on the objectives of software development (GSRM) which explicitly incorporates the requirements engineering phase. This model allows for preventing, assessing, treating and monitoring the risk from the expression of the objectives thereof. The main limitations of this model are that it is unsuitable for large projects and does not take into account the specific context of the project. Van der Aalst and al. [24] proposes a method for risk management by the configuration of indicators. This method suffers mainly from its limitation in the single case study of the risks that can cause project delays.

Given these shortcomings, this paper proposes a workflow-based mining approach that ensures the achievement of project objectives (cost, quality, time), adapted to every project and taking into account the environment in which it s executes.

3. CONCEPTS

In this section, the major modeling concepts of risk management in a project are defined. The presentation of these concepts is given using the denotational semantics [27]. These concepts are largely derived from the modeling method ATSERO [4] and are certain continuity thereof.

3.1 The task

A task is the atomic activity which cannot be divided into smaller tasks. Performing a task transforms the state of the environment in another. In this study, a task is formally considered as follows :<nt; pre; post; QoSa> where s is the name of the task, pre is a non empty set of preconditions, post is a non-empty set of post-conditions and QoSa the quality of service expected of this task.

Définition 1: (Task action)

Let E = <J, S, val>, a given state s t and a task that satisfies the precondition in s, then the action of t in s is denoted ts specified by ts = {o: J, s (o) ≠ t (s) (o)}. When there is no ambiguity, a task will be represented by its name t, pre (t) and post (t) is the precondition and post conditions respectively. Based on the post condition of a task t and state s where s (post (t)) = true, assuming that ts = + post (t) U -post (t).

3.2 Quality of service

Quality of Service QoS is rated service performance which determines the level of satisfaction provided to the beneficiaries of these services. The level of satisfaction is defined as the set of properties, criteria, characteristics and performance of services provided to customers. In addition, many jobs are done in this area, each defining a specific set of specific criteria to measure QoS. In the literature, there is still no consensus on the definition of a common set of criteria for evaluating QoS. The evaluation criteria are defined in terms of objectives and specific requirements of each organization. In this part of the work, the definition of an abstract model that provides the semantics of QoS is done.

QoS is defined by (cost, time, quality, Val, f, g, h) where cost is the financial cost of the project, within the assigned time period, as a magnitude scale from 0-20 describing the project, f defined function cost: →val g defined function delay: →val, h the function defined by quality: → val.

3.3 Experience

Experience noted Exp can be defined by :

Exp = (NbAnnees, NbProjets, Diploma)

WhereNbAnnees is the number of years of work by the resource, NbProjets is the number of projects in which he participated and Diploma is the highest degree.

3.4 The resource

There are many types of agents participating in the execution of tasks in an information system. They perform tasks to complete certain missions which in turn add a dimension to the quality of service. A resource in an information system can be a human actor, equipment, function (program) or a given. A resource is formally defined by Ress = (Id, Exp, Log) where Id set identifier, Exp is experience; log is the log file of the resource.

3.5 The event

An eventnoted Ev is modeled by Ev = (Id, Task, Res_used, Task_action, QoS_obtain) with id the identifier of the event, the executed task, Res_used the resource used for the execution of the task, Task_action the Action of the task, the quality of service QoS_obtain obtained after execution of the task.

3.6 The Log

The log or journal is the file containing all the events occurring in a project. Formally log = (Ev-set).

3.7 Workflow

A workflow is formally defined by (Task-set, Ress, QoS_obtain, f, g) where Task-set is a set of tasks, Ress is a set of resources, QoS_obtain is the quality of service obtained, the function f as Task :→Ress and g function as Task * Ress: →QoS_obtain

Définition2 :

QoS obtained (QoS_obtain) in a workflow is equal to the sum of qualities of service received from the workflow tasks. More formally, QoS_obtain = Σ Ev (Qos_obtain).

3.8 The risk

The risk [5] is defined as the uncertainty in achieving the objectives. Its formal definition Risk = <SR, NR; IdR; Vr; Dom; Csk; NIVR; Prio; Av; Resa; Resp> where SR is the set of risk sources (example: delay, lack of human resources, etc.), NR is the name of risk IdR is the identifier of risk, Vr is an integer that represents the likelihood of occurrence of this risk, Dom is the area of impact, Csk is the set of likely consequences in case of occurrence of the risk of identifying IdR, NIVR is an integer that represents the level of this risk, Prio is an integer that indicates the priority level of risk, Av is the set of opportunities that the risk is booking all expected by the process of managing this risk, Resp results is the set of responsibilities (resources) incurred by the risk.

3.9 Knowledge

Knowledge is a set of similar and usable information for action. It is generally resulting from the sum of knowledge and experience acquired over time. Knowledge can be formally defined by: = Know Ulog (Ress_i * Exp).

3.10 The environment

The environment Env is formally defined by (Know-set, Task-set, Ress-set) where Know-set is a set of knowledge, task-set is a set of tasks and Ress-set is a set of resources that are responsible for the execution of all tasks.

3.11 The Project

Project [19] is a temporary exercise in order to create a product or a service or a single result effort. The temporary nature of projects implies a beginning and an end determined. The end is reached when the project objectives are met, or when the project is stopped because its objectives will not be achieved or may not be, or when the project is no longer useful. As part of this work, the project is considered a workflow associated with a threshold of acceptability (range defining criteria satisfiability objectives) and its formal definition is Pr = <Wf; SA; Env, f> where Wf is the workflow executed by the project, the SA threshold of acceptability and f: Wf→ SA.

NB: SA the acceptability threshold is defined by [QoSmin; QoSmax] with QoSminQoSmax and the quality of service expected and minimally and maximally respecting the following property: ∀q QoS_ = TkQoSmin ≤ ≥ q qQoSmax with the quality of service obtained after executing the task Tk.

Définition3:

Both projects are "similar" if they have the same execution environment and the sameacceptability threshold.

The following commutative diagram elucidates the interactions between the concepts mentioned above. Writing A → B means that from an element A, we can obtain all the elements of B attached to it. The transitivity property is respected, that is to say, if A → B and B → C, then A → C.

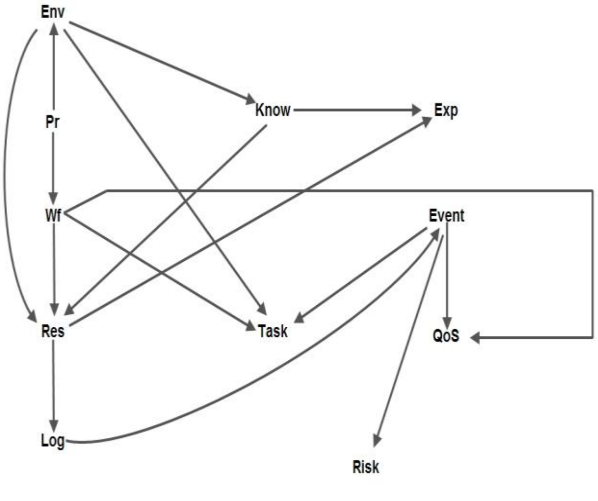

Figure 3: Commutative diagram of concepts

4. CONTRIBUTION TO RISK MANAGEMENT

In this section, the model of risk management in a proposed project is based on the workflow mining previously presented. The presentation of that model begins with a definition of political risk management, the normative model of the project, the descriptive model of the project. Then all the salient points of this model are solved.

4.1 Security Risk Management Policy

The management policy determines how to assign resources to tasks based on their quality of service associated (time, cost, and quality). Based on the problem of risk management, management policy is based on concepts that teks task, resource, quality of service, project workflow. The concept of task identifies all activities attributable to resources. The concept of resource is used to list all the resources likely to receive permission to perform a task. The concept of quality of service identifies the set of criteria satisfiability of performing a task, workflow concept is a set of tasks performed to produce a service, the concept of the project is a workflow which can be assigned an acceptability threshold. Based on these concepts, the Management Policy (RMP) can be defined as follows:

- ✶ $QoS_{TK} = Task \rightarrow QoS$
- ✶ $QoS_{PROJ} = Pr \rightarrow QoS$
- ✶ $QoS_{Wf} = Wf \rightarrow QoS$
- ✶ *TASKRES = Ress→Task-set*

4.2 Normative Model of the project

Pursuant to the management policy defined above and without any external action that violates it, the project model is that defined by project managers in the analysis phase and is normative model of the project. Formally, it can be defined as:

Prnor = <Pr; SRMP> where Pr is the target project and SRMP is the security Risk Management Policy. The normative model describes how the project must be executed in conformity with the policy. The actual situation of project implementation is given below in the descriptive model.

4.2 Descriptive Model of the projet

This model describes the project as activities take place within it based on the events of all tasks performed, all associated resources and quality of service obtained in the different activities of the system. Workflow in a project actually expresses the interactions between project stakeholders standing out the EventLogs. In this approach, no activity is saved, it is taken into account in the normative approach of the project or not. Thus the actual situation of the project is described with her condition. Model Description is formally defined by Prdes = <Pr; Runs> where Pr is the target project, Runs all the events that satisfy the trigger conditions for the execution of tasks.

4.3 Risk IdentificationModel

Risk identification is to identify all the risks that may affect the project and documenting their characteristics. In this work, the risk is considered to be the gap between the normative model and the descriptive model. Thus, the identification of risk IR model is defined as follows:

$IR = Ulog_{DES}(Ress\_i) \backslash SRMP.$

4.4 Processing Model and risk response plan

The treatment is the action to take vis-à-vis a risk to minimize its impact in accordance with the policy set management. It is defined as: Tr = <De; AcT> From where is the decision to treat or not that risk is AcT processing action stopped for this risk. The response plan is the risk element of the risk management plan that lists the risks, and risk associated with each treatment. Formally, it can be defined as PRR = <IR; Tr; g> where IR is the set of identified risks, Tr is the set of treatments, a function g such that g: IR -> Tr.

5. CONCLUSION AND FUTURE WORKS

The need for risk management is demonstrated for all types of projects, especially for major projects that are intended pillars of the achievement of emergence objectives of some countries including Cameroon. Unfortunately, the methods of risk management now widely used are not above reproach and clearly see their limits this due to their "speculation" [29] with the notion of risk associated to a project. A new way to do based on the richness of the past, to clearly assess the risks involved in a project of a given type is proposed in this paper. The proposed model is based on the workflow mining to extract knowledge about risk fled in past projects. We observe the prescriptive and descriptive models to extract the resulting gap. This gap is a list of significant risks in future projects of the same type. This model has the advantages described formally identifying risks, treatment associated with a risk and beyond the risk response plan. The description of the process of writing the plan risk response using hidden algebra makes it a major advantage because it takes into account the risk treatment never occurred, which is innovative in terms of risk management. To improve the results of this work and to better manage the risks in IT projects in the near future, the project will be divided into sub-set of tasks that will be seen as services. We can thus define a "Service Architecture Structure" in which the various services will be shared through the use of proclets.

6. REFERENCES

[1] Standish Group. The Standish Group Report - CHAOS. Project Smart, 2014.

[2] Barry W. Boehm. Software risk management: Principles and practices. IEEE Software, 8(1):32–41, 1991.

[3] Shareeful Islam. Software Development Risk Management Model- a goal-driven approach. PhD thesis, TechnischeUniversitatMunchen, March 2011.

[4] Roger AtsaEtoundi. "atsero method : a guideline for business process and workflow modelingwithin an entreprise". International Journal of Scientific Engineering Research, 2, December 2011.

[5] ISO 31000 – Risk Management Standard, page 2, February 2008.

[6] H. Knight. (1921) Risk, Uncertainty and Profit. [Online]. www.econlib.org/library/Knight/knRUP.html

[7] Amine NEHARI TALET, Razali MAT-ZINand Maaradj HOUARI. Risk Management and Information Technology Projects.International Journal of Digital Information and Wireless Communications, (IJDIWC) 4(1): 1-9,2014.

[8] Southern, S, "Creating risk management strategies for IT security," *Network Security*, pp. 13-14, 2009.

[9] J. Kontio, "The Riskit Method for Software Risk Management version 1, 00," University of Maryland. College Park, MD, Computer Science Technical Reports CS-TR-3782 / UMIACSTR- 97-38, 1997.

[10] Boehm, B., & Bose, P., "A collaborative spiral software process model based on theory W", in *3rd International*

Conference on the Software Process (ICSP94), New York, 1994.

[11] Higuera.R&Haimes.Y, "Software Risk Management", Software Engineering Institute Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, Technical Report CMU/SEI-96-TR-012 ESC-TR-96-012, 1996.

[12] Etoundi Roger, Atsa, Onanena Georges, Nkoulou, Mi Bahanag Nicolas, Nkondock,&MoyoAchille, M. (2013). A Formal Framework for Intrusion Detection within an Information System based on Workflow Audit. *International Journal of Computer Applications*, *81*(1), 1-10.

[13] S., Feather, M., & Hicks, K. Cornford, "DDPTool for life-Cycle Risk Management. Jet Propulsion Laboratory," CalifornaiaInstitutte of Technology, IEEE, 2001.

[14] J., Jurison, "Software project management: The manager’s view," *Communications of Association for Information Systems*, vol. 2, no. 17, pp. 2-52, 1999.

[15] Bandyopadhyay, K., Myktyn, P., &Myktyn, K., "A framework for integrated risk management in information technology",*Management Decision*, pp. 437-444, 1999.

[16] Bruckner, M., List, B., &Schiefer, J., "Risk-Management for Data Warehouse Systems," *Data Warehousing and Knowledge*, pp. 219-229, 2001.

[17] Beck, T., Levine, R., Loayza N., "Finance and the Sources of Growth",*Journal of Finance and Economics*, vol. 58, pp. 261-300, 2000.

[18] P. & Merritt, G. Smith, "Proactive Risk Management: Controlling Uncertainty in Product Development",*Productivity Press, New York*, 2002.

[19] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, 4th ed., 2008. [Online].http://www.projectsmart.co.uk/pdf/pmbok.pdf

[20] Sommerville. I, *Software Engineering*, 8th ed. University of St. Andrews, United Kingdom: Addison-Wesley,2006.

[21] Software & Systems Engineering Standards Committee of the IEEE Computer Society, "Systems and software engineering — Life cycle processes — Risk management," International Organization forStandardization/International Electrotechnical Commission, ISO/IEC 16085 IEEE Std 16085-2006.

[22] TOGAF. (2009) The Open Group Architecture Framework (TOGAF). [Online]. http://www.kingdee.com/news/subject/10togaf/pdf/TOGAF_9_ziyuan.pdf

[23] J. Herbst L. Maruster1 G.Schimm W.M.P. van der Aalst, B.F. van Dongen and A.J.M.M.Weijters. "workow mining: A survey of issues and approaches.

[24] C.J. Fidge A.H.M. terHofstede A. Pika, W.M.P. van der Aalst and M.T. Wynn. Profilingevent logs to configure risk indicators for process delays. International Conference onAdvanced Information Systems Engineering (Caise 2013), Springer-Verlag, volume 7908 ofLecture Notes in Computer Science: 465–481, 2013.

[25] K. Vergidis A. Tiwari A.K. Jallow, B. Majeed and R. Roy. Operational risk analysis in business processes. BT Technology Journal, 25(1):168–177, 2007.

[26] R.C. Lunardi L.Z. Granville L.P. Gaspary J.A. Wickboldt, L.A. Bianchin and C. Bartolini.A framework for risk assessment based on analysis of historical information of workflowexecution in it systems. Computer Networks, 55(13):2954–2975, 2011.

[27] R.D. Tennent. The denotational semantics of programming languages ii. Communicationof the ACM, 1976.

[28] Joseph A. Goguen. Hidden Algebra for software Engineering. University of California at San Diego, La Jolla CA 92093-0114 USA.

[29] Victoria Montgomery. New statistical methods in risk assessment by probability bounds.PhD Thesis, Durham University, UK, February 2009.