Computer Networks 55 (2011) 2954–2975

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A framework for risk assessment based on analysis of historical information of workflow execution in IT systems

Juliano Araujo Wickboldt [a,*], Luís Armando Bianchin [a], Roben Castagna Lunardi [a], Lisandro Zambenedetti Granville [a,*], Luciano Paschoal Gaspary [a], Claudio Bartolini [b]

[a] Institute of Informatics, Federal University of Rio Grande do Sul, Av. Bento Goncalves, 9500, CEP 91.509-900, Porto Alegre, RS, Brazil
[b] Hewlett Packard Laboratories, Palo Alto, USA

ARTICLE INFO

Article history:
Received 23 December 2010
Received in revised form 17 May 2011
Accepted 29 May 2011
Available online 24 June 2011

Keywords:
Infrastructures and services management
Risk management
Change management
Project management
Networks operations and management

ABSTRACT

Services provided by modern organizations are usually designed, deployed, and supported by large-scale IT infrastructures. In order to obtain the best performance out of these services, it is essential that organizations enforce rational practices for the management of the resources that compose their infrastructures. A common point in most guides and libraries of best practices for IT management – such as ITIL or COBIT – is the explicit concern with the risks related to IT activities. Proactively dealing with adverse and favorable events that may arise during everyday operations might prevent, for example: delay on deployment of services, cost overrun in activities, predictable failures of handled resources, and, consequently, waste of money. Although important, risk management in practice usually lacks in automation and standardization in IT environments. Therefore, in this article, we introduce a framework to support the automation of some key steps of risk management. Our goal is to organize risk information related to IT activities providing support for decision making thus turning risk response planning simpler, faster, and more accurate. The proposed framework is targeted to workflow-based IT management systems. The fundamental approach is to learn from problems reported in the history of previously conducted workflows in order to estimate risks for future executions. We evaluated the applicability of the framework in two case studies both in IT related areas, namely: IT change management and IT project management. The results show how the framework is not only useful to speed up the risk assessment process, but also to assist the decision making of project managers and IT operators by organizing risk detailed information in a comprehensive way.

1. Introduction

In order to deliver high quality services to customers, modern organizations often end up employing large-scale Information Technology (IT) infrastructures, typically composed of physical and logical heterogeneous resources such as routers, firewalls, servers, end-user hosts, network protocols, and software packages. As IT services are designed, deployed, maintained, and improved, organizations can run into problems, for example, of scalability and complexity of management. To achieve better outcome from provided services and avoid waste of substantial resources, rational practices in the management of IT infrastructures must be enforced. To this end, some best practice standards and libraries have been published, aiming to provide guidance for proper IT management. Two of the most widely recognized guides are the Information Technology Infrastructure Library (ITIL) [1] – proposed by the Office

* Corresponding authors. Tel.: +55 (51) 9861 1336; fax: +55 (51) 3316 7308 (J.A. Wickboldt).
E-mail addresses: jwickboldt@inf.ufrgs.br (J.A. Wickboldt), labianchin@inf.ufrgs.br (L.A. Bianchin), rclunardi@inf.ufrgs.br (R.C. Lunardi), granville@inf.ufrgs.br (L.Z. Granville), paschoal@inf.ufrgs.br (L.P. Gaspary), claudio.bartolini@hp.com (C. Bartolini).

1389-1286/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2011.05.025

of Government Commerce (OGC) – and the Control Objectives for Information and related Technologies (COBIT) [2] – introduced by the Information Systems Audit and Control Association (ISACA).

An explicit concern of the IT management guides is related to the necessity of managing risks associated with an organization's IT activities. This is emphasized by the fact that both OGC and ISACA have published specific documents for corporative IT risk management: the Management of Risk (M_o_R) [3] from OGC, and the Risk IT [4] from ISACA. According to M_o_R, to achieve their objectives, organizations must necessarily take a certain amount of risk. It is thus the role of the risk management discipline to help organizations to methodologically deal with risks associated with their activities.

Usually, organizations take risks as uncertain events or conditions that, if happen, may affect the accomplishment of business goals. Those events, along with the conditions that represent risks to the business, should be identified and assessed in terms of probability of occurrence and possible impact to the business objectives. Although the literature recommends tackling both negative (threats) and positive (opportunities) effects of risks, in practice, negative effects are far more considered in real IT environments. This results in current risk management practices being in fact strongly focused on the prevention and mitigation of harm.

The risk management discipline is based on four logically sequential and cyclic processes [3]: (i) *identification* of possible threats and opportunities to the objectives of a given organizational activity, (ii) *assessment* of identified risks in terms of probability of occurrence and associated impact (*i.e.*, estimation of possible losses or earnings), (iii) *response planning* for preventive and reactive responses to identified risks, aiming to minimize threats and enhance opportunities, and (iv) *implementation and monitoring* of the planned responses in order to tackle risks, evaluate the effectiveness of preventive actions, and occasionally dispatch corrective ones. Along all these processes, it is important that organizations adopt a common set of internal policies and strategies for risk management to be shared among their departments and teams. Some of these policies and strategies, for example, may define tolerance thresholds, scales for estimating probabilities and impacts, and tools for documenting, reporting, and communicating risks.

Despite all best practices and recommendations, the experience of practitioners shows that there is little evidence that risk management is being efficiently applied in a systematic and repeatable way. In fact, standard guides like ITIL or COBIT only provide high level guidelines for general purpose risk management in a textual descriptive form. Very few information is given about how to actually implement these standards in practice and most of the proposed processes are assumed to be manual. Recently, some authors have investigated the actual benefits and shortcomings of different approaches for risk management in real-life environments [5–7]. These investigations expose many issues of current risk management actual practices, such as inadequate documentation, little knowledge reuse, and lack of tools to automate, report, monitor, and support decision making. In the end, the quality of risk-related decisions is often too much dependent on the experience of IT managers. The current practice on risk management usually encompasses an excessive dependency on people, thus becoming a time/resource consuming, occasionally counterproductive task.

Considering the today's actual risk management scenario, we emphasize that one of the major problems in risk management is the lack of automation and system-assisted routines. In this research, we pay special attention to problems in the *risk assessment* process, in which risks are tackled in terms of probability of occurrence and possible impact. The risk assessment process is usually based on interviews and brainstorms with involved stakeholders, in a very *ad hoc* fashion. Since the quality of risk related decisions and response planning depends directly on the accuracy of risk assessment, the employment of automated tools to assist IT managers in achieving more precise estimations becomes a key factor for the success of risk management as a whole.

Several authors have been investigating ways to support risk management in specific contexts or situations [8–13]. In previous investigations of our research group, we have also proposed punctual solutions to enable some degree of automation in estimating probabilities and impacts in risk assessment [14–16]. Our main goal in this article is to consolidate the approaches previously proposed into one single unified framework to support the automation of key processes of risk management, aiming to make it simpler, faster, and more accurate. The proposed framework is based mostly on best practices proposed in the aforementioned standards and libraries (*e.g.*, ITIL and M_o_R). In this work, we focus on risk assessment for workflow-based systems designed for the management of IT infrastructures and services. There are many types of IT management processes that can be modeled in the form of workflows, such as change management, project management, portfolio management, and incident management. The advantage of using workflows lies in the fact that they define a sequence of fine-grained activities to be executed in a given order and the details of the execution of these activities (including reports of adverse and favorable events) can be recorded to logs for further analysis. Our approach encompasses the automated analysis of logs of previously executed workflows in order to learn from events reported in the past, aiming to help in the design of better workflows for future execution.

In order to prove the concept of our solution, two case studies are taken from two IT related areas, namely *IT change management* and *IT project management*. The former presents general guidelines for consistently conducting changes over IT infrastructures, from the early specification, planning, and deployment, towards evaluation and review [17]. The latter is focused on the design phase of services, aiming to ensure that a project meets its objectives avoiding waste of resources [18,19]. These areas are relevant in the context of IT infrastructures and services management since they have received much attention from both academy and industry in recent years. Moreover, both projects and changes can be organized in the form of workflows and therefore may have their risks assessed using the unified framework proposed in this work.