ABSTRACT

This work focuses on issues typically encountered in organizations whose core business largely depends on ICT: continuous monitoring, continuous auditing, controlling and assessment of transactions risk. Organizations have been making efforts to implement methods and systems which enable them to increase reliability of their business and, simultaneously, to be in accordance with their organizational objectives and compliant with external regulations. Thus, this work presents and validates an innovative solution to implement Continuous Assurance services in information systems applicable to any organizational transaction, regardless of its type, dimension, business area or even its information system support technology. This last objective is pursued having as support an ontological model at an abstraction level that guarantees that independence. This research culminated with the development of a prototype and consequent results analysis, using data collected from the near-real implementation, allowing us to ensure the feasibility and the effective use of the proposal.

Keywords: Continuous Assurance, Enterprise Information Systems, Management Information System, Organizational Transactions, Risk Profiles

DOI: 10.4018/ijeis.2015010102
INTRODUCTION

Currently, organizations are facing several challenges resulting from evolving business models pressured by factors as the new ICT (Information and Communication Technologies) trends and changing conditions in the environment. As an example, their organizational transactions have grown in volume and complexity. In addition, they are living in highly regulated business environments (Marques, Santos & Santos, 2013c) and are exposed to several threats and risks (Alan & Allen, 2005). Thus, controlling and monitoring are needed in order to evaluate and validate all transactions, in a comprehensive manner, to meet regulation demands. However, the data size and time response requirements related to this new environment make the traditional audit process, which occurs mostly after the completion of transactions, inefficient. Hence, for many organizations there is a significant risk of errors and fraud and these are not detected in time, resulting in a negative impact for organizations (Askary, Goodwin & Lanis, 2012). See, for example, the current global financial crisis and successive well-known scandals in some organizations, such as Lehman Brothers, A-Tec, Madoff, Kaupthing Bank, WorldCom, Enron, Parmalat and Tyco cases and many others. Thereby, automatic mechanisms will make it possible to mitigate the risk associated to these issues (Bodoni, 2014; Markham, 2006). Furthermore, the continuous monitoring of the behavior of enterprise systems is becoming apparent, since it allows to detect problems in run-time and to solve them before they negatively affect business (Shuchih & Boris, 2008).

The trend for improvement and strengthening of risk control structures has grown due to the increasing emergence of new regulatory requirements in this area. These structures provide greater security in the effectiveness of risk management activities, ensuring an appropriate management of business risks and the effective operation of internal control systems (Pereira & Mira da Silva, 2012; Spies & Tabet, 2012). Consider, for example, Sarbanes-Oxley Act (SOX), which is one of the most well-known regulations in this area (Li, Peters, Richardson & Weidenmier Watson, 2012). Prior to SOX, there were other models and frameworks of reference, such as the COSO (Committee of Sponsoring Organizations of the Treadway Commission) and COBIT (Control Objectives for Information and related Technology) (Lankhorst, 2013; Prawitt & Tysiac, 2013). In Europe measures for the statutory auditing were also taken by Directive 2006/43/CE of the European Parliament and of the Council of 17th May 2006, helping to improve the integrity and efficiency of financial statements and, accordingly, enhance the orderly functioning of markets.

Organizations must be sufficiently prepared to survive, regardless of exposure and of the large number of risks they are subject to, by implementing an adequate mechanism to implement Continuous Assurance in accordance with applicable legislative and regulatory framework. Continuous Assurance is defined as a set of services that using technology and data transactions produces audit results immediately or within a short period of time after the occurrence of relevant events (Vasarhelyi, Alles & Williams, 2010).

There is another aspect to consider in relation to organizational transactions: risk profiles. In this context, risk profiles refer to the classification of different types of behavior that may occur in the execution of a transaction. In this work, two terms are considered to characterize risk profiles: negative profiles, which refer to all unwanted behaviors during the execution of transactions, for example incomplete or poorly executed operations, lack of crucial procedures, non-conformities, delays, incongruities and malfeasace; and positive profiles, which refer to all valid and appropriate events (Santos, 2009).

It is necessary to find solutions which allow organizations to continuously evaluate, monitor and validate their transactions, preferably in a non-intrusive way concerning business
A Case Study of a Government-Sponsored Enterprise Resource Planning Project in a Chinese Apparel Company
www.igi-global.com/article/case-study-government-sponsored-enterprise/74373?camid=4v1a