Chapter 5
Continuous Assurance and Business Compliance in Enterprise Information Systems

Rui Pedro Marques
University of Aveiro, Portugal & University of Minho, Portugal

ABSTRACT

The increase of reliability and compliance of business processes is currently a major concern of organizations which simultaneously intend to achieve their organizational objectives and be compliant with external regulations. Thus, organizations are frequently looking for methods, tools and solutions which enable them to improve business compliance, and reduce the likelihood of situations that may jeopardize their operational performance and corporate image. This chapter aims to bring together a set of results and conclusions from a research project whose purpose was to conceptualize and validate an innovative solution which simultaneously monitors and audits organizational transactions executed in Enterprise Information Systems. A prototype was developed and deployed in a near-real environment. From the results, we conclude that the prototype offers Continuous Assurance services and is applicable to any organizational transaction, regardless of its type, dimension, business area or even its information system support technology. This independence is guaranteed by the abstraction level of an ontological model which is used to represent the organizational transaction we intend to monitor and audit. A case study enabled us to confirm the feasibility and effectiveness of the proposal in business compliance.

INTRODUCTION

Currently, organizations are living in a very regulated and competitive business environment. This, along with the challenges resulting from evolving business models pressured by factors as the new ICT (Information and Communication Technologies) trends and changing conditions in the environment, has forced organizations to reinvent themselves. Furthermore, the volume and complexity of business processes and the different threats and risks they are exposed to (Alan & Allen, 2005) have spurred or-

DOI: 10.4018/978-1-5225-2382-6.ch005

ganizations to look for solutions which enable them to control and monitor their transactions, evaluating and validating them in a comprehensive manner in order to meet current demands.

However, the traditional auditing, which occurs mostly after the completion of transactions, has proven inefficient, increasing the likelihood of errors and fraud not detected in time, and 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).

There are some regulatory requirements and risk control structures which help and encourage organizations to strengthen effectiveness of their 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). The most well-known regulation in this area is SOX (Sarbanes-Oxley Act). COSO (Committee of Sponsoring Organizations of the Treadway Commission) and COBIT (Control Objectives for Information and Related Technology) are the most used reference frameworks. 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.

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 operations. The optimization of the operational performance will also be possible if this auditing is done in real time (in the shortest time possible after any relevant event occurrence), reducing in this way the associated risks (Arnold & Sutton, 2007; Lech, 2011). Thus, the adoption of appropriate mechanisms to implement Continuous Assurance in accordance with applicable legislative and regulatory framework is crucial for organizations to be sufficiently prepared to survive, regardless of exposure and of the large number of risks they are subject to. Continuous Assurance can be 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).

This chapter presents the results and conclusion of a research project (Marques, Santos & Santos, 2015) whose main objective was the development of real-time assurance services, having as support the organizational transactions according to an ontological model of organizational transactions. The use of an ontological model in this project was important because it helped to understand the essence of the organizational transactions and their relationships and characteristics, allowing the independence that is needed to make the project applicable to any organizational transaction, regardless of its type, dimension, business area or even its information system support technology. In parallel, even from a simpler business view, detachment from any ontological representation results in the inability to generate organizational knowledge (Filipowska, Hepp, Kaczmarek & Markovic, 2009).

The ontological model used in this project was the 'Enterprise Ontology', proposed by Dietz (2006). This model is adapted to represent the essential structure of the organizational transactions, with no significant complexities but simultaneously with: coherence (i.e. parts constituting an integral whole); consistency (there is no contradiction or irregularities); comprehension (all the important issues are