Chapter 22
Aiding Compliance Governance in Service-Based Business Processes

Patrícia Silveira
University of Trento, Italy

Carlos Rodríguez
University of Trento, Italy

Aliaksandr Birukou
University of Trento, Italy

Fabio Casati
University of Trento, Italy

Florian Daniel
University of Trento, Italy

Vincenzo D'Andrea
University of Trento, Italy

Claire Worledge
Deloitte Conseil, France

Zouhair Taheri
PricewaterhouseCoopers Accountants, The Netherlands

ABSTRACT

Assessing whether a company's business practices conform to laws and regulations and follow standards and SLAs, i.e., compliance management, is a complex and costly task. Few software tools aiding compliance management exist; yet, they typically do not address the needs of who is actually in charge of assessing and understanding compliance. We advocate the use of a compliance governance dashboard and suitable root cause analysis techniques that are specifically tailored to the needs of compliance experts and auditors.

The design and implementation of these instruments are challenging for at least three reasons: (1) it is fundamental to identify the right level of abstraction for the information to be shown; (2) it is not trivial to visualize different analysis perspectives; and (3) it is difficult to manage and analyze the large amount of involved concepts, instruments, and data. This chapter shows how to address these issues, which concepts and models underlie the problem, and, eventually, how IT can effectively support compliance analysis in Service-Oriented Architectures (SOAs).

DOI: 10.4018/978-1-61350-432-1.ch022

INTRODUCTION

Compliance generally refers to the conformance to a set of laws, regulations, policies, best practices, or service-level agreements. *Compliance governance* refers to the set of procedures, methodologies, and technologies put in place by a corporation to carry out, monitor, and manage compliance. Compliance governance is an important, expensive, and complex problem to deal with:

It is *important* because there is increasing regulatory pressure on companies to meet a variety of policies and laws (e.g., Basel II, MiFID, SOX). This increase has been to a large extent fueled by high-profile bankruptcy cases (Parmalat, Enron, WorldCom, the recent crisis) or safety mishaps (the April 2009 earthquake in Italy has already led to stricter rules and certification procedures for buildings and construction companies). Failing to meet these regulations means safety risks, hefty penalties, loss of reputation, or even bankruptcy (Trent, 2008).

Managing and auditing/certifying compliance is a very *expensive* endeavor. A report by AMR Research (Hagerty et al., 2008) estimated that companies would have spent US$32B only on governance, compliance, and risk in 2008 and more than US$33B in 2009. Audits are themselves expensive and invasive activities, costly not only in terms of auditors' salaries but also in terms of internal costs for preparing for and assisting the audit – not to mention the cost of non-compliance in terms of penalties and reputation.

Finally, the problem is *complex* because each corporation has to face a large set of compliance requirements in the various business segments, from how internal IT is managed to how personnel is trained, how product safety is ensured, or how (and how promptly) information is communicated to shareholders. Furthermore, rules are sometimes vague and informally specified. As a result, compliance governance requires understanding/interpreting requirements and implementing and managing a large number of control actions on a variety of procedures across the business units of a company. Each compliance regulation and procedure may require its own control mechanism and its own set of indicators to assess the compliance status of the procedure (Bellamy et al., 2007).

If we look at how every-day business is being conducted at an operative level, we note that technologies like web services and business process management systems have largely proved their viability for organizing work and assisting and orchestrating also human actors involved in business processes. The adoption of the so-called *service-oriented architecture* (SOA) to conduct business (eased by technologies such as SOAP, WSDL, and HTTP) has further affirmed the analogy between web service technologies and common business practices, turning the traditional, heavyweight and monolithic software approach into flexible and reconfigurable service ecosystems. One of the advantages of this kind of ecosystem is that they suddenly allow one to obtain fine-grained insights into runtime aspects, e.g., message exchanges, events, and process progress states, which can only hardly be accessed in traditional legacy systems. As we will see in this chapter, in our work we specifically leverage on this potential in order to check compliance of service-based business processes.

Interestingly, despite these novel opportunities, compliance is to a large extent still managed by the various business units in rather ad-hoc ways (each unit, line of business, or even each business process has its own methodology, policy, controls, and technology for managing compliance) and without leveraging on the new transparency of electronic business (Sloane et al., 2006). As a result, nowadays it is very hard for any CFO or CIO to answer questions such as: *Which rules does my company have to comply with? Which processes should obey which rules? Which processes are following regulations? Where do violations occur? Which processes do we have under control?* (Cannon & Byers, 2006). Even more, it is hard to do so from a perspective that not only satisfies