Chapter 18
Integrating Compliance Management in Service-Driven Computing:
Conceptual Models and Automation Architecture

Natallia Kokash
Centrum Wiskunde and Informatica (CWI), The Netherlands

ABSTRACT

The lack of effective controls over organizational business processes can cause serious consequences for a company's reputation and even jeopardize its existence. There is a need for continuous monitoring of controls and systematic collection and evaluation of relevant data. Compliance management is essential for ensuring that organizational business processes and supporting information system are in compliance with laws, regulations, and various legislative or technical documents pertaining to the place of business. The focus of this chapter is to provide an insight into compliance management and discuss the integration and automation of compliance management in service-driven computing. The chapter elaborates conceptual models for specifying compliance requirements originating from various sources and details aspects such as multi-view process modeling annotated with compliance requirements, annotation of service interfaces and behavioral characteristics, development and reuse of compliant process fragments, architectural patterns to simplify compliance management, and abstract frameworks to ensure compliance in the context of service-driven computing through service adaptation and run-time governance. Finally, approaches to automating compliance management through formalization of compliance requirements, rule- and event-based monitoring, and integration of compliance governance systems with automated reasoning and verification tools are detailed.

DOI: 10.4018/978-1-4666-6178-3.ch018

INTRODUCTION

Compliance management is essential for ensuring that organizational business processes and its supporting information systems are in accordance with a set of prescribed requirements originating from laws, regulations, and various legislative or technical documents such as Sarbanes-Oxley Act (SOX), ISO 17799, Solvency II, Basel III, etc. As the violation of such requirements may lead to significant punishment for an organization, compliance management should be taken into consideration very seriously. Compliance requirements in principle affect all stages of software development, from the very early stages of business process design to the regular maintenance and upgrade of deployed systems of a functioning organization.

The notion of compliance is often confused with the notion of conformance which is a more traditional and widely used term in software engineering. While there can be debates about the meaning and scope of both terms, roughly the difference can be summarized as follows:

- **Conformance:** Measures how well a given implementation matches or does not match a standard or a reference. For example, a specification may require the implementation of a secure connection for online payment operations.
- **Compliance:** A broader concept that aims to measure how well an organization or an entire industry functions to achieve specific high-level goals prescribed by law or regulatory documents. For example, among such goals can be to avoid frauds, improve safety, etc.

Compliance documents rarely aim at constraining technical aspects of the IT infrastructure; they do not provide ready-to-use solutions or enforce specific technical protocols. Conformance of a company's software to rules or guidelines derived from compliance documents may be part of achieving compliance with the initial regulation, but it alone cannot guarantee the company's compliance. Similarly, if a company is in compliance with some legislative document (e.g., one that implements internal control on financial reporting prescribed by the SOX), it does not imply that its software is conformant to any technical standard, protocol, or a reference. It can comply with best practices in some aspects (e.g., all Web services conform to the WS-I basic interoperability profile) and fall short, or differ in other areas (e.g., browsers used by company's staff do not support TLS encryption).

With all the benefits regulatory documents bring, official jurisdictional documents are often confusing, contradictory, and require specially trained people to understand, interpret, implement and monitor them for possible changes and editions. The more generic a regulation is, the more ways exist to unintentionally violate it. Joint efforts of an organization's management team, lawyers, accountants, IT consultants, auditors, software developers, and quality assurance specialists are required to develop a compliant IT infrastructure. Thus, rather than considering compliance as a state, we should think of compliance as a never ending process of adhering to the guidelines or rules established by external bodies such as government agencies or internal corporate policies.

At a glance, compliance documents encourage companies to centralize and automate their systems. The advantage of centralized and automated systems becomes apparent when the comparative costs of companies with decentralized operations and systems, versus those with centralized systems are analyzed. For example, according to the annual reports on SOX Section 404, compliance costs have continued to decline relative to revenues since 2004, mainly due to the automation of controls (Sweeney, 2012; Protivity, 2012; Whalen et al., 2010). However, the cost for decentralized companies (i.e., those with multiple segments or divisions) is still considerably higher than those of centralized companies. Thus, the