Chapter 11
Semantic Policies for Modeling Regulatory Process Compliance

Marwane El Kharbili
University of Luxemburg, Luxemburg

Elke Pulvermueller
University of Osnabrueck, Germany

ABSTRACT

Business process management (BPM) as a paradigm for enterprise planning and governance is nowadays a core discipline of information systems management. Growing up from the first process re-engineering initiatives in the 1980's, BPM technologies now seek to span all of the organizational silos of enterprises, and also expand vertically from the strategy layers where visions and goals are defined to the lower data transaction layers. Ensuring the compliance of processes to the guidance and control provided to the business by regulations is an obligation to every enterprise. In this work, we motivate the need for automation in compliance management and propose the use of policies as a modeling concept for regulations. We introduce the CASE model for structuring regulatory compliance requirements as policies. Policies shall allow to model regulations at abstraction levels adequate to implementing platform independent mechanisms for policy verification. We describe the CASE model and explain how it can be used to structure and model policies extracted from regulations. This chapter also defines a policy modeling ontology that we propose as a language for formally modeling CASE policies. The basic CASE model and the corresponding policy modeling ontology support compliance of enterprise processes to regulations by enabling automation to compliance checking (verification). The utilization of the CASE method as well as the policy ontology is showcased using an example of resource access control in business processes.

DOI: 10.4018/978-1-4666-2919-6.ch011

INTRODUCTION

Business Process Management (BPM) is the discipline of capturing, modeling implementing, and controlling all activities taking place in an environment defining the enterprise, and this, in an integrated manner (Scheer, 2000). Organizations do not only own business processes, they are also subject to regulations. Not being compliant to regulations diminishes the added-value business processes represent for the organization, e.g. through non-optimal alignment with (i) quality standards, (ii) business partner service agreements or (iii) non-identified security flaws (El Kharbili et al., 2008a). Non-compliance to regulations could also be the cause of judiciary pursuits, as in the case with laws such as the Sarbanes-Oxley Act (SOx, 2002), which, among other aspects, seek to impeach financial manipulations in order to protect stakeholders in a company.

Consequently, non-compliance has both short-term (e.g. cost savings, reduced governance complexity) and long-term (e.g. judiciary pursuits, market confidence) consequences. Compliance management is the term covering all activities and methods to ensure that a company follows all guidance and implements all measures required by an external or internal regulation (El Kharbili et al., 2008a). By extension, compliance management also refers to standards, frameworks, and software used to ensure the company's observance of legal texts. In the context of BPM, compliance management applies on business processes and the related resources like data and systems. Business processes are typically inter-departmental by nature. Similarly, inside organizations, compliance management spans the spectrum of horizontal activities (e.g. IT security or quality standard compliance) that are inter-departmental and inter-organizational by nature. Non-compliance at the level of business processes is critical because business processes control all value adding activities of a company. A comprehensive compliance management framework for Business Process (BP)-centered enterprises should take this aspect into account and permit hiding the complexity of BPs from compliance experts in order to concentrate efforts on what should be checked instead of how it should be checked.

A framework allowing organizations to integrate regulatory compliance tasks with business process management presents many advantages, as we will show. There exists a very high interest in the issues tackled by this work within the scientific community. Large projects like Compas (Compas, 2010) and Master (Master, 2010) illustrate this, for instance.

Requirements on such a framework have already been elicited in (El Kharbili et al., 2008a) and in more systematic and analytical fashion in (Ly et al., 2008) as well as a high-level architecture proposed in (El Kharbili et al., 2008a). Our approach to designing such a framework is based on policies. We argue that policies supported with semantic descriptions of business processes present many advantages for our purpose with regard to modeling, knowledge management and enforcement as well as monitoring.

More than the need for automation and complete coverage of enterprise models in compliance management, formal modeling of compliance is a requirement when considering the need for verification and validation of modeled compliance measures. Also automated compliance management implies compliance checking functionalities. In the following sections of this chapter, we will show how policies and rules as enterprise model artifacts can be used for fulfilling these requirements. In our work, we assume that an enterprise model is process-centered (as with ARIS (Scheer, 2000)), and as such, we seek to model compliance on semantically modeled BPs which are used as the elements connecting enterprise model artifacts. This is for instance the approach taken by the SUPER project (SUPER, 2010a). Our work will also lead us to introduce an extension of the