An Integrated Solution for Runtime Compliance Governance in SOA

Aliaksandr Birukou[1], Agnieszka Betkowska Cavalcante[2], Fabio Casati[1], Soudip Roy Chowdhury[1], Vincenzo D'Andrea[1], Frank Leymann[3], Ernst Oberortner[4], Jacek Serafinski[2], Patricia Silveira[1], Steve Strauch[3], and Marek Tluczek[2,⋆]

[1] DISI, University of Trento, TN 38123, Italy
[2] Telcordia Poland, Poznan
[3] IAAS, University of Stuttgart, 70569, Germany
[4] Distributed Systems Group, Vienna University of Technology, 1040, Austria

Abstract. Compliance governance in organizations has been recently gaining importance because of new regulations and the diversity of compliance sources. In this demo we will show an integrated solution for runtime compliance governance in Service-Oriented Architectures (SOAs). The proposed solution supports the whole cycle of compliance management and has been tested in a real world case study.

Keywords: compliance governance, DSL, monitoring, SOA, CEP.

1 Introduction and Contributions

Compliance governance refers to the overall management approach for controlling the state of compliance in the entire organization and, in general, consists of: (1) selecting the sources to be compliant with and designing corresponding compliance requirements; (2) (re-)designing business processes compliant with the selected requirements; (3) monitoring compliance of processes during their execution; (4) informing interested parties (managers, auditors) on the current state of compliance; (5) taking specific actions or changing the processes in cases of (predicted or happened) non-compliance. Compliance governance has been gaining importance in organizations because of new regulations appeared recently (e.g., Sarbanes-Oxley Act, Basel III, Solvency II), non-compliance bringing money loss and reputation damage, and the diversity of compliance sources: business owners consider legislature and regulatory bodies, standards and codes of practice, business partner contracts. Existing approaches rarely deal with different types of compliance sources and cover only few steps of the compliance governance.

In this demo we will show how service-oriented technology can be used as the basis for an integrated solution for runtime compliance governance in a company.

⋆ This work was supported by funds from the European Commission (contract no. 215175 for the FP7-ICT-2007-1 project COMPAS).

P.P. Maglio et al. (Eds.): ICSOC 2010, LNCS 6470, pp. 706–707, 2010.

The framework includes tools for: modeling compliance requirements for different compliance sources in domain-specific languages; linking the requirements to the business processes; monitoring process execution using Complex Event Processing (CEP); displaying the current state of compliance in dashboards, and analyzing cases of non-compliance to find what caused them. The framework is targeted at people dealing with compliance in an organization, ranging from people specifying compliance requirements (process analysts, compliance officers, technical specialists) to those controling the compliance (managers, auditors) and it helps them to deal with various compliance aspects in a uniform and automated manner. The framework has been applied in a real case study in the context of the EU FP7 project COMPAS[1] (Compliance-driven Models, Languages, and Architectures for Services). The case study focuses on the compliance of telecom service provider to licenses of its business partners. The framework provides the following unique contributions:

- handling requirements from different source in a uniform manner within an integrated solution;
- covering whole compliance governance lifecycle;
- the model-driven approach reduces user inputs by transforming information defined in requirements to further steps - up to monitoring;
- supporting traceability and access to information during runtime execution, monitoring and mining, thus enabling drill-down in non-compliant cases.

2 Demonstration Storyboard

The live demonstration introduces the contributions of the compliance governance framework by means of a joint use of slides (for the conceptual aspects) and hands-on framework demos (for the practical aspects):

1. Advanced Telecom Services scenario: a company provides customers with on-demand aggregated audio/video streaming by combining services from different providers
2. Design aspects: identifying compliance sources and requirements, modelling business process, expressing compliance requirements in QoS and Licensing Domain-Specific Languages (DSLs), generating events and CEP rules for monitoring.
3. Runtime aspects: deployment of the process in the process engine, executing the process, showing the use of the online dashboard for monitoring and the offline dashboard for the historical analysis of the processes.
4. Runtime Compliance Governance architecture: explanation of the architecture and showing that framework in general is more than what is shown in the demo.

The video illustrating this demo is available at
`http://disi.unitn.it/~birukou/2010runtime-compas-demo.zip`

[1] `http://www.compas-ict.eu`