CoReL: Compliance Representation Language

Marwane El Kharbili
Laboratory for Advanced Software Systems
University of Luxembourg
marwane.elkharbili@uni.lu

1 Introduction

Compliance management has received considerable attention in recent years in both industry and in research [4]. In the industry, awareness grew dramatically after several scandals starting in 2001 and the ENRON fraud which is directly correlated with the advent of the Sarbanes-Oxley Act (SOx, 2002) [2]. Markets now shifted towards a tighter regulatory control of economic activities, through a wide variety of regulations to be implemented by organizations (e.g., drugs and food, healthcare). The cost of achieving regulatory security compliance for example is on average 3.5$ million each year per company in the U.S.A., according to a survey of 160 individuals leading the IT, privacy and audit efforts at 46 multinational organizations done in 2011 [3].

Compliance is especially important in the context of business processes (BPs) [5]. After analyzing industrial solutions to the management of regulatory compliance, we distinguish two main approaches: (i) compliance audits, and (ii) software implementations. While both solution categories suffer from high costs related to the external expertise that must be acquired by the enterprise, they present different disadvantages and advantages [2].

Compliance audits are hard to automate since they require human intervention. Moreover, audits are error-prone and do not cover the whole enterprise model as they are conducted on samples of process logs or on selected parts of the information system. Software approaches are inflexible and are not generic, i.e. these are usually specifically targeted at one compliance problem and hard to be reused for other types of problems. Additionally, both approaches are so-called reactive approaches, since they do not enable early discovery and handling of situations eventually leading to violations before the latter happen [6]. Finally, it is a challenge to find adequate solutions supporting the full regulatory compliance lifecycle shown in Figure 1 (see the right side), as the mechanisms needed for each phase of the lifecycle are different. For instance, many approaches only tackle verification (i.e., static checking of compliance models) and do not tackle monitoring (i.e., dynamic checking of compliance models). On Figure 1, the dashed lines show that some phases of the BPM and RCM life-cycles must be aligned.

Model-driven engineering group. Laboratory for Advanced Software Systems. Computer Science and Communications Unit.

2 Research Design

Many attempts have been made in research at providing both usable and tractable, as well as powerful and expressive solutions for supporting compliance initiatives in BPs. However, most of these solutions focus on the challenge of formally describing compliance requirements in order to automatically verify them [4]. The focus is not put on real end users of compliance frameworks, who are business-users and no computer scientists, making for low acceptance of novel solutions from research. Our objective is to tackle this issue and provide an adequate paradigm for regulatory compliance management (RCM) that is suitable to business users.

We reckon through analyses of typical compliance management scenarios and existing research on the topic that automation, support of the full BPM/RCM lifecycle, as well as pro-active compliance management are valuable capabilities that an RCM framework should provide[7, 4]. Our research seeks to achieve the previous three capabilities by answering the research questions listed in Table 1. In order to do that, we study the semantic gap between the conceptual terms in which business users think about compliance and the ones needed for a formal representation of compliance. A new modeling language is needed for creating reusable, lower-complexity and business-user friendly compliance models. The most important criterion is that the language semantics support both automatic verification as well as enforcement of compliance requirements at the push of a button.

The usability claims are validated by showing how to integrate our language with two different business process modeling notations and applying the language to a case study. The ontological expressiveness of our language is evaluated by comparing it with existing frameworks (e.g., [1]). Finally, field studies are conducted using the modeling language with users with no previous knowledge of formal methods.

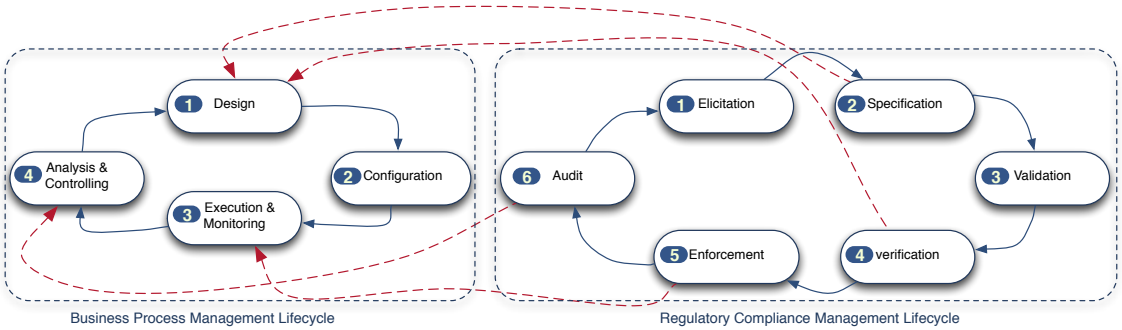

Figure 1: The lifecycle of regulatory compliance management

Table 1: Research Questions

ID	Research Question
	Modeling
1	How to make RCM Modeling amenable to Business Users?
2	How to deal with logical formalism weaknesses?
3	How to cover several enterprise business aspects (EBAs)?
4	How to be usable with various BPM notations?
	Checking
5	How to realize 'verification' using compliance models?
6	How to realize 'monitoring' using compliance models?

3 Results & Conclusion

This research contributes the visual compliance representation language (CoReL) and the framework around it. CoReL is a domain specific modeling language, and is based on the core concept of *business policy*, which we propose to fill the semantic gap between business users and formal methods. Business policies allow to model decision-making by breaking it into reusable parts [5]. They allow to reason about all possible violation types and how to adequately react to each of them depending on a number of factors such as the current context. Business policies exist at a different conceptual level from business rules and therefore allow to flexibly combine rules written in different types of formalisms[1] combining both structural and temporal aspects.

We defined formal operational semantics for CoReL for both authorizations and obligations [5]. We define a further graphical rule modeling language which allows reusing rules easily from a rule library embedded in the definition of CoReL business policies.

By relying on the theory of formal model driven engineering, we are able to use model composition to integrate CoReL into two widely used notations[2] [5].

Model transformations allow to generate different formal representations of both the CoReL business policies as well as the process models referred to by the business policies. Using model checking as a verification technique, we are able to do time-efficient compliance verification (i.e., static checking) [5].

This has the advantage of using a so-called 'push-button' technique, appreciated for its simplicity of use. By also using model transformations, we are also able to enforce business policies during process execution[3] [5].

The research outlined here proposes a novel perspective on the problem of RCM, which places business users at the center and proposes a visual modeling language named CoReL. It leverages model-driven engineering theory to automate the verification and enforcement phases. The perspectives opened by this work include, among others, extending the framework to assist with violation localization and explanation.

[1]E.g., a temporal rule language like LTL and a constraint language like OCL

[2]We used the eEPC and BPMN modeling languages

[3]Our underlying formal model relies on algebraic petri nets

4 References

[1] T. D. Breaux. *Legal Requirements Acquisition for the Specification of Legally Compliant Information Systems*. PhD thesis, North Carolina State University, Raleigh, North Carolina, USA, April 2009.

[2] M. El Kharbili and E. Pulvermueller. A Semantic Framework for Compliance Management in Business Process Management. In *Proceedings of the 2nd BPSC'09-SABRE*, LNI, pages 60–80. GI, GI, March 2009.

[3] N. W. Ellen Messmer. Cost of regulatory security compliance? - on average, $3.5m., 05.10.2012.

[4] M. Kharbili. Business process regulatory compliance management solution frameworks: A comparative evaluation. In A. Ghose and F. Ferrarotti, editors, *Asia-Pacific Conference on Conceptual Modelling (APCCM 2012)*, volume 130 of *CRPIT*, pages 23–32, Melbourne, Australia, 2012. ACS.

[5] M. E. Kharbili, Q. Ma, P. Kelsen, and E. Pulvermueller. CoReL: Policy-based and model-driven regulatory compliance management. In *Proceedings of the 15th IEEE EDOC*, pages 247–256, 2011.

[6] S. Sadiq and G. Governatori. Managing regulatory compliance in business processes. In *Handbook on Business Process Management 2*, page 175. 2010.

[7] N. Syed Abdullah, S. Sadiq, and M. Indulska. Emerging Challenges in Information Systems Research for Regulatory Compliance Management. In *CAISE*, volume 6051 of *LNCS*, chapter 21, pages 251–265. 2010.