Towards a comprehensive design-time compliance management

El Gammal, A.; Turetken, O.; van den Heuvel, W.J.A.M.; Papazoglou, M.

Published in:
Proceedings of the 15th International Business Information Management Conference (IBIMA 2010)

Publication date:
2010

Towards a Comprehensive Design-time Compliance Management: A Roadmap

Amal Elgammal, Ph.D. Candidate, Tilburg, The Netherlands, a.f.s.a.elgammal@uvt.nl
Oktay Turetken, Post-doc Researcher, Tilburg, The Netherlands, o.turetken @uvt.nl
Willem-Jan van den Heuvel, Professor, Tilburg, The Netherlands, w.j.a.m.vdnheuvel @uvt.nl
Mike Papazoglou, Professor, Tilburg, The Netherlands, m.p.papazog@uvt.nl

Abstract
Today's business climate demands business processes to meet many compliance regulations that require all enterprises to review their processes and ensure that they satisfy the set of relevant compliance requirements. Compliance management should be considered from the very early stages of business process design, thus achieving compliance by design. In this paper, we give a brief overview of an approach for managing business process compliance during design-time phase of business process lifecycle. We also discuss the roadmap for the key components and their relationship for a comprehensive design-time compliance support.

Keywords: Regulatory compliance, Design-time compliance management, Business process management.

Introduction
Compliance to regulations, such as Basel II and Sarbanes-Oxley (SOX) has become one of the major concerns of organizations. *Compliance* is mainly ensuring that business processes, operations and practices are in accordance with a prescribed and/or agreed on set of norms (Sadiq et al., 2007), namely *compliance requirements*. There is an increase in the number of regulations, standards, legislations and other sources of compliance requirements, which enforce organizations to assess their business processes and make sure that they adhere to the constraints set forth. Thus, a comprehensive compliance management solution is of utmost importance, which must support compliance throughout all the stages of the business process lifecycle staring from the design phase. Without effective and powerful compliance frameworks and approaches, organizations face litigation risks and even criminal penalties.

As a part of the work to develop a comprehensive solution to support business process compliance in all phases of the business process lifecycle, we have introduced a framework to manage business process compliance during *design-time*. The framework constitutes key components including an approach, tools and techniques as well as their relationships to address the challenges for achieving 'compliance-by-design'. The framework also helps to identify the key challenges and open research problems in this field. In the next sections, we summarize the overall *approach* for design-time business process compliance management briefly zooming in on its major components. We also summarize key studies on design-time compliance specification, verification and analysis. Finally, conclusions are highlighted.

Design-time Business Process Compliance Approach
In general organizations achieve compliance on a per-case basis typically as ad-hoc solutions. These solutions are generally handcrafted for a particular compliance problem, which raises several difficulties particularly from software architecture perspective. The solutions are hard to maintain and evolve as they usually involve hard-coded requirements across multiple systems. Their reusability is also limited since they are custom made for a particular problem. Decoupling business process logic from compliance requirements that restrict the way the processes run is one of the first steps that helps to manage and evolve business processes and compliance requirements

that are more likely to change over time. Decoupling involves the specification and management of compliance requirements and all relevant concepts as a separate entity -starting from abstract requirements to concrete and organization-specific rules- and requires them to be linked to the relevant business processes to enable their *traceability*. In addition to this motive, one of the main objectives of the approach for design-time compliance is to be able to apply formal process verification techniques during design-time, which enables us to automatically check business process specifications against formally specified compliance requirements.

Fig. 1 depicts important aspects and key components of the proposed approach for design-time business process compliance. There are two primary roles involved in this approach: (i) a *business expert*, who is responsible for defining and managing business processes in an organization while taking compliance requirements into account, and (ii) a *compliance expert*, who is responsible for the internalization, specification and management of compliance requirements stemming from external and internal sources in close collaboration with the business expert. The approach encompasses two logical repositories; the *business process repository* and the *compliance requirements repository*, which are semantically aligned via shared domain ontology. Process models are defined and maintained in the business process repository, while the compliance requirements and all relevant concepts are defined, maintained and organized in the compliance requirements repository. The approach assumes the overall process to start either from the business process side (the right-hand side of Fig. 1) or from the compliance requirements side (left part of Fig. 1). Process models can be specified in the Business Process Execution Language (BPEL); the de-facto standard for workflows that provides an XML-based language to describe the operational logic of the process and its execution flow. However, as BPEL is not grounded on a formal model, BPEL specification should be transformed into a formal representation, e.g. some variant of a finite state automaton (e.g. Buchi automata (Buchi, 1960)) to enable the verification of these business process specifications against formally specified compliance rules. Other process modeling languages and notations, such as Business Process Modeling Notation (BPMN), can also be used for this purpose. However, the extent of the compliance requirements that can be verified is depended on the expressiveness of the language used for the specification of the business process.

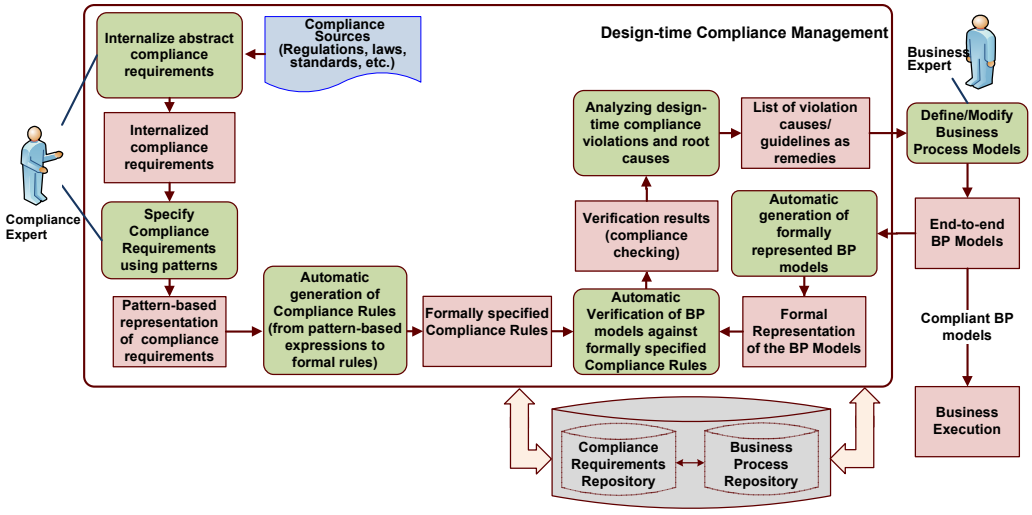

Fig. 1. Design-time compliance management framework

On the other side, the *internalization* of abstract compliance requirements originating from regulations, policies, standards and other compliance sources into a set of organization-specific, concrete norms requires not only compliance but also business process domain knowledge. There are only few approaches that help organizations to go through this process. The procedure we introduce is based on the COSO (COSO, 1994) framework and briefly involves the following major steps:

- Identification of the objectives and the abstract requirements enforced by the compliance sources with which the organization has/agrees on to comply.
- Performing 'risk assessment' to identify the risks to the achievement of these objectives/abstract requirements imposed by the compliance sources.
- Identifying, designing and implementing 'controls' to mitigate the identified risks. Controls are concrete and organization-specific norms to be verified, enforced or tested in order to ensure that compliance requirements are satisfied.
- Specifying formal compliance rules for those controls that can be formally represented and be used for process verification at design-time and later phases.

In general, logical languages that can be used for the formal specification of compliance requirements, e.g. Linear Temporal Logic (LTL), Computation Tree Logic (CTL) are difficult to be used and understood by users. The complexity of these powerful languages represents the main obstacle for utilizing the associated sophisticated analysis and reasoning tools. To solve this problem, the framework offers *patterns* for compliance expert to use as an intermediary step between these requirements and formal statements. The pattern-based expressions are then automatically transformed into the adopted logical language. As shown in Fig. 1, the inputs to the 'automated verification' component are; the formally specified end-to-end business process models; and the formally specified compliance rules. E.g. automatic verification can be supported by 'model checkers', e.g. SPIN model checker (Holzmann, 1997), which enable the verification of properties formally specified as LTL formulas against a system that is formally specified as a Buchi automata (Buchi, 1960). In case of violations, verification results can direct the business expert in modifying the business process model for the resolution of the violation. The business process models are updated and re-mapped to their formal forms and finally re-verified against the set of applicable compliance requirements. This process iterates continuously until no violations are detected.

Design-time Compliance Specification and Analysis

To help to manage the evolution of compliance requirements and their internal/external traceability, these requirements should be represented at various levels of abstractions to accommodate with various stakeholders needs, starting from sources and moving down to their formal representations. The existence of a physical constraints repository is vital for this purpose. Studies in (Breaux et al., 2006) and (Giblin et al., 2005) propose interesting solutions for maintaining the *traceability* between various levels and important related concepts. On the other hand, an automated verification of business process models against a set of relevant compliance requirements requires these requirements to be based on a formal foundation of an expressive logical language. *Deontic logic* (e.g. FCL (Governatori et al., 2006)) and *temporal logic* (e.g. LTL (Liu et al., 2007)) families have been successfully utilized in the literature as the formal foundation of compliance requirements. In (Elgammal et al., 2010 to appear), we report a comparative analysis between deontic and temporal logics based on the capabilities and limitations of each language and a set of identified features. Once business and compliance specifications are formally represented, automated verification tools can be applied to check the compliance. If temporal logic is used as the formal foundation of compliance requirements, model-checkers can be utilized for this purpose. Key work examples in this direction are: (Giblin et al., 2005), (Liu et

al., 2007), (Yu et al., 2006) and (Schumm et al., 2010 (to appear)). On the other hand, if deontic logic is utilized, associated reasoners can be exploited for design-time verification. For example, *Idealness* notions are defined in (Governatori et al., 2006) to verify the compliance, where Formal Contract Language (FCL) is used as the formal foundation of compliance requirements. Key work examples utilizing languages based on Deontic logic are: (Sadiq et al., 2007), (Governatori et al., 2006), (Goedertier and Vanthienen, 2006) and (Milosevic et al., 2006).

Furthermore, assisting the user to resolve non-compliance during design-time is an important issue that has not been paid much attention from the research community. Obviously, indicating whether a compliance requirement is satisfied or not is not sufficient. The counter-example tracing facility, typically provided by model-checkers, can aid users by highlighting the fragments in the business process model that are the sources of non-compliance. However, a more intelligent feedback is still required, which contains a set of rationale explaining the underlying reasons why the violation occurred and what strategies can be used as remedies. In (Elgammal et al., 2010 - to appear), we propose a root-cause analysis approach for design-time compliance violation on the basis of property patterns. Other key studies in this direction are in (Ghose and Koliadis, 2007), (Lu et al., 2008) and (Awad et al., 2009).

Conclusion

Business processes form the foundation for all organizations, and as such, are impacted by industry regulations. Without explicit business process definitions, effective and expressive compliance frameworks, organizations face litigation risks and even criminal penalties. Compliance management should be one of the integral parts of business process management, which should crosscut the complete business process lifecycle, starting from the very early stages of business process design. Design-time compliance management should be further integrated with runtime monitoring, e.g. (Namiri and Stojanovic, 2007), and offline monitoring of the complete business process instances, e.g. (Aalst et al., 2005), thus providing a lifetime compliance support. In this paper, we present a very brief overview of a comprehensive design-time compliance management framework. We can conclude that providing such a comprehensive support brings about several challenges, as it requires a cross-disciplinary approach and the existence and integration between various components, tools and techniques.

Acknowledgment

This work is a part of the research project “COMPAS: Compliance-driven Models, Languages and Architectures for Services”, which is funded by the European commission, funding reference FP7-215175.

References

AALST, W., BEER, H. & DONGEN, B. 2005. Process Mining and Verification of Properties: An Approach based on Temporal Logic. *International Conference on Cooperative Information Systems (CoopIS’05).* Cyprus.

AWAD, A., WEIDLICH, M. & WESKE, M. 2009. Specification, Verification and Explanation of Violation for Data Aware Compliance Rules. *7th International Conference on Service Oriented Computing (ICSOC- Service Wave'09).* Springer.

BREAUX, T., ANTON, A. & SPAFFORD, E. 2006. A Distributed Requirement Management Framework for Legal Compliance and Accountability. Technical Report, Dept. of Computer Science, North Carolina State Univ.

BUCHI, K. 1960. On a Decision Method in Restricted Second Order Arithmetic. *International Congress on Logic, Method, Philosophy of Science.* Stanford.

COSO 1994. Internal Control – Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission. .

ELGAMMAL, A., TURETKEN, O., VAN DEN HEUVEL, W. & PAPAZOGLOU, M. 2010 - to appear. Root-Cause Analysis of Design-time Compliance Violations on the basis of Property Patterns. *8th International Conference on Service-Oriented Computing (ICSOC10).* USA.
ELGAMMAL, A., TURETKEN, O., VAN DEN HEUVEL, W. & PAPAZOGLOU, M. 2010 to appear. On the Formal Specification of Business Contracts and Regulatory Compliance. *4th Workshop on Formal Languages and Analysis of Contract-Oriented Software.* Pisa, Italy: EPTCS.
GHOSE, A. & KOLIADIS, G. 2007. Auditing Business Process Compliance. *Service-Oriented Computing – ICSOC07.* Austria.
GIBLIN, C., LIU, A., MULLER, S., B., P. & ZHOU, X. 2005. Regulations Expressed As Logical Models. *18th International annual conference of legal knowledge and information systems.* Belgium.
GOEDERTIER, S. & VANTHIENEN, J. 2006. Designing Compliant Business Processes with Obligations and Permissions. *the International Business Process Management Workshops (BPM).* Austria.
GOVERNATORI, G., MILOSEVIC, Z. & SADIQ, S. 2006. Compliance Checking Between Business Processes and Business Contracts. *10th International enterprise distributed object computing conference (EDOC 2006).* Hong Kong
HOLZMANN, G. 1997. The Model Checker SPIN. *IEEE Transactions on Software Engineering* 23**,** 279 - 295.
LIU, Y., MULLER, S. & XU, K. 2007. A Static Compliance-Checking Framework for Business Process Models. *IBM Systems Journal,* 46.
LU, R., SADIQ, S. & GOVERNATORI, G. 2008. Measurement of Compliance Distance in Business Processes. *Information Systems Management* 25**,** 344-355.
MILOSEVIC, Z., SADIQ, S. & ORLOWSKA, M. 2006. Translating business contract into compliant business processes. *10th IEEE International Enterprise Distributed Object Computing Conference.* Hong Kong.
NAMIRI, K. & STOJANOVIC, N. 2007. Pattern-based Design and Validation of Business Process Compliance. *Lecture Notes in Computer Science***,** 59-76.
SADIQ, S., GOVERNATORI, G. & NAIMIRI, K. 2007. Modeling Control Objectives for Business Process Compliance. *10th International Conference on Business Process Management.* Australia.
SCHUMM, D., TURETKEN, O., KOKASH, N., ELGAMMAL, A., LEYMANN, F. & VAN DEN HEUVEL, W. 2010 (to appear). Business Process Compliance through Reusable Units of Compliant Processes. *1st International Workshop on Engineering SOA and the Web (ESW'10).* Austria: LNCS.
YU, J., MANH, T., HAN, J. & JIN, Y. 2006. Pattern-Based Property Specification and Verification for Service Composition. *7th international conference on web information systems engineering (WISE06).* China.