Towards a Framework for Semantic Business Process Compliance Management

Marwane El Kharbili[1], Sebastian Stein[1], Ivan Markovic[2], Elke Pulvermüller[3]

[1] IDS Scheer AG, ARIS Research
Altenkesseler Str. 17, 66115 Saarbrücken, Germany
marwane.elkharbili@ids-scheer.com
sebastian.stein@ids-scheer.com

[2] SAP Research Center CEC Karlsruhe, SAP AG
Vincenz-Prießnitz Str. 1, 76131 Karlsruhe, Germany
ivan.markovic@sap.com

[3] Institute of Computer Science, University of Osnabrück
Albrechtstr. 28, 49076 Osnabrück, Germany
elke.pulvermueller@informatik.uni-osnabrueck.de

Abstract. Processes count to the most important assets of companies. Ensuring the compliance of processes to legal regulations, governance guidelines, and strategic business requirements is a sine qua non condition to controlling business behavior. Implementing business process compliance requires means for modeling and enforcing compliance measures. In this work, we motivate the need for automation in compliance management and introduce the role of policies. We then distinguish eight requirements for a compliance management framework. We also discuss different ways of conducting compliance checking. Finally, we propose a policy-based framework for business process compliance management. We eventually proceed to a discussion of the soundness and practicability of our approach, followed by an investigation of the main challenges ahead of our approach to policy-based semantic business process compliance management.

Keywords: Compliance Management, Business Process Management, Policy, Business Rule, Ontology.

1 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 [4], [5]. Several languages, frameworks, and tools that support one or many of the listed aspects are available. 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[1].

Non-compliance to regulations can also be the cause of judiciary pursuits as many financial scandals in recent years have shown[2]. This has happened in the US and in Europe as the examples of both Enron [2] and Parmalat show. It is due to these scandals that laws and legal guidelines have been designed, in order to protect companies and their stakeholders from manipulations of financial reporting data [3]. 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 referring to the definition of means to avoid such illegal actions by controlling an enterprise's activities. 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 support and realize value-adding activities inside companies. Inside organizations, compliance management spans the spectrum of horizontal activities (e.g. IT security or quality standard compliance). Hence, compliance to regulations must also be ensured at the level of business processes. Non-compliance at the level of business processes is critical because business processes control all value adding activities of a company. There are many regulations and their scope varies from financial reporting to security. Fig. 1 gives an idea about this variety:

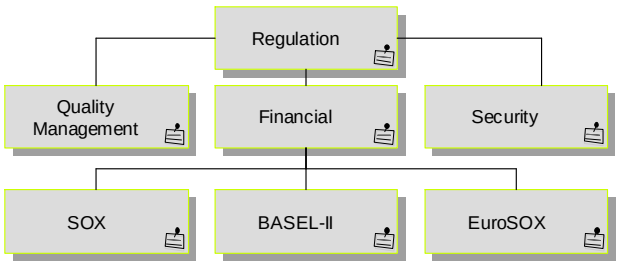

Fig. 1. A concept map of some regulations.

SOX[3] [10] is one of the legislations that generate most reactions in the form of numerous research on compliance, because companies doing business in the US are obliged to implement it and also because of its high implementation costs [1]. SOX was passed in 2002 after the Enron financial scandal. Sections 302 (Certification of

[1] Non-identified security leaks can drop the overall quality of the business processes by making them vulnerable to malicious attacks.

[2] We refer to the financial scandals at corporations like Enron, WorldCom, Roche, Siemens, and Volkswagen.

[3] The "Public Company Accounting Reform and Investor Protection Act" is also known as the Sarbanes-Oxley act. SOX is an usual abbreviation for this act.

Disclosure in Companies' Quarterly and Annual Reports) and 404 (Definition of Internal Controls over Financial Reporting) of SOX are IT-related and thus explain the focus of computer science academia on both sections [3]. The European equivalent to SOX is called EuroSOX and was passed by the European commission in 2006. BASEL-II is a proposal[4] by the Basel committee that seeks to align regulatory capital requirements with operational and credit risk [6], [7]. ISO/IEC 27002:2005[5] [9] is the internationally recognized standard for IT security and acts as a regulation when defining security policies. Finally, ISO 20000 is an example of quality standard.

A framework allowing organizations to integrate regulatory compliance tasks with business process management presents many advantages as we will show. Our approach to designing such a framework is based on policies. We argue that policies present many advantages for our purpose, especially when supported with semantic descriptions of business processes. In the following, we proceed to a further discussion of the problem in section 2. In section 3, we define eight requirements for our compliance management framework, discuss several forms of conducting compliance checking, and make a high-level proposal for a business process compliance framework. Section 4 contains a review of related work. We conclude with section 5, where we discuss challenges upfront and future work.

2 Problem Discussion

As shown in Fig. 2, regulations are transformed into measures adapted to the enterprise. Compliance measures are usually implemented using procedures, policies, and controls. The latter are documented and communicated in natural language. This, of course, makes discovering inconsistencies or contradictions a hard task. Even ensuring that all roles involved in the compliance management project have the same understanding of the policies to be enforced is a hard task, since regulations are on purpose kept very abstract to stay independent from their implementation. Moreover, an organization does not have continuous information about its compliance status. This concern is particularly relevant when regulations are subject to change. Companies need to be able to easily ensure compliance with new versions of regulations. This is the reason why hard-coded compliance measures are the source of high costs for compliance-aware organizations. Moreover, companies go through audits in order to be certified as being compliant with a regulation. But such an approach to compliance management has high costs, because such audits have to be performed on a regular basis.

The risks at stake for a company that eventually does not get successfully audited as compliant to a regulation can be severe, ranging from penal consequences on management level (e.g. in case of financial reporting fraud, according to SOX) or to

[4] Made by the Basel Committee on Banking Supervision.
[5] Previously ISO/IEC 17799 [8].

lost contracts with clients (e.g. clients requiring a certain certification[6] that the company could not be audited positively for). Compliance management is still a discipline relying heavily on manual, error-prone, sample-based procedures undertaken by auditors, i.e. the level of automation in governance, risk, and compliance projects is still very low.

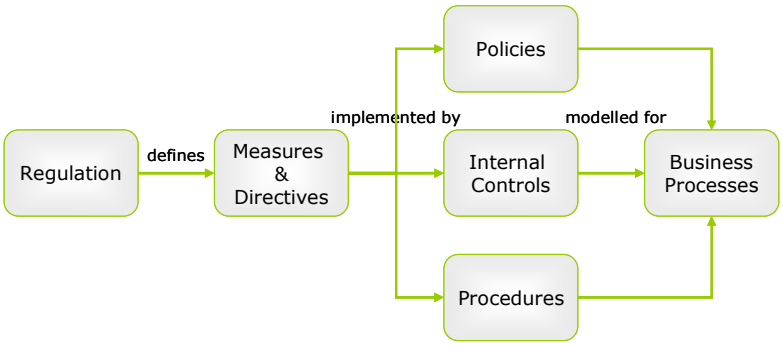

Fig. 2. A basic high-level model for regulatory compliance

Additionally, auditors must have the necessary expertise and know-how to lead compliance checking projects on a certain system or a whole organization, with regard to a certain regulation. This means companies seeking to ensure their business processes' regulatory compliance must manage separate projects for each type of regulation (see Fig. 1). Moreover, having a sound knowledge of (i) the regulations to be compliant with and (ii) of the processes that are part of the scope of a compliance management project is a necessary condition for successful compliance. This is why compliance management projects also involve experts from the audited organization. Thus, companies dealing with several regulatory texts and laws face an increasing complexity in both managing regulatory knowledge and compliance enforcement on business processes. Auditors cannot check the whole process landscape. They take samples, selected previously to the actual audit. This way, no preliminary internal audits can take place unless the organization has an internal compliance team, which generates additional costs to the organization. A framework for integrated compliance management would minimize the resources required to realize internal audits and logically increase success chances before the actual audit. Furthermore, the accuracy and coverage of regulatory compliance is increased through automated-checking the whole scope of business processes.

Processes do not just span multiple vertical sections of a single enterprise, but can also span multiple enterprise boundaries (cross-enterprise process/service choreography). Therefore, compliance management processes have to include mechanisms enabling them to deal with such complexity. Another more holistic approach is the following: regulations are destined to be enacted on the complete

[6] It is a common practice that companies ask business partners (suppliers, distributors, and outsourcing partners) to be certified, e.g. with regard to quality norms. Many companies realize certification audits on business partners themselves.

enterprise model, not only on business processes. In order to fully implement compliance management, it should more generally act on enterprise models. Several standard frameworks for enterprise models exist such as TOGAF [14], the Zachman framework ([13], [15] and [16]) and ARIS [4]. Similar work on semantic enterprise models such as [17] has also been conducted.

As by nature, regulations are in their original form very abstract specifications. This is mainly for two reasons:

(i) Keeping regulations abstract means ensuring more independence from implementation and more flexibility in adapting regulations to different business problems. See for example ISO 20000 or ISO 27001 (quality and security respectively).

(ii) The writers and users of regulations are business people and lawyers. Their instrument of work is natural language and is non-formalized. This language often incorporates domain specific terminology, as well as structures and definitions that can barely be fully understood by non-domain specialists.

This is why a regulation's semantics can be understood and implemented in different manners, by different departments of the same organization or across different organizations involved. Again, this can slow down compliance management measures and make them inconsistent and thus inefficient. Semantic consistency of the data and of the definition of regulations must be achieved. We see semantics in the form of ontologies as the solution to this challenge. A semantic representation provides the flexibility and extensibility needed for modeling continuously evolving regulations. It also allows a declarative implementation of compliance checking through the use of inference engines that are designed for the ontology language used.

Formal modeling of regulations and policies for business processes makes formal representation of business processes a necessity, too. Semantic business processes fulfill this requirement. Ontologies for business process modeling can be extended with ontologies for regulation and policy modeling, in one word "compliance ontology". Ultimately, these ontologies would allow the use of inference engines in order to discover non-compliant configurations and behavior of business processes. The same approach could be used to further enforce these policies if the ontologies are designed to support that. It is thus a fundamental requirement to work with a comprehensive semantic business process model. A semantic framework for BPM that is designed to optimize and querying the process space is introduced in [11]. Ontologies for the description of business processes would allow coupling business process definitions with semantic regulatory compliance definitions. In [12], such an approach is proposed.

In the following chapter, we focus on defining requirements for a business process regulatory compliance framework. We also distinguish different approaches to the implementation of semantic compliance checking and finally come up with our own proposal for a compliance framework.

3 A framework for compliance management

In order to design the framework, we first define general requirements on a compliance management framework in section 3.1. We will further distinguish 5 perspectives under which compliance checking can be observed in section 3.2. After, we describe an architecture that fulfills the previously defined requirements.

3.1 Eight requirements for a compliance management framework

We discussed in section 2 some problems related to compliance management. For example, we have explained why semantic consistency of the modeled regulations is important and what costs compliance audits generate for companies. From the experience we have in the field of governance, risk and compliance, we have identified eight dimensions to assess the value of an approach to compliance management. We present these in the form of requirements as shown in Fig. 3.

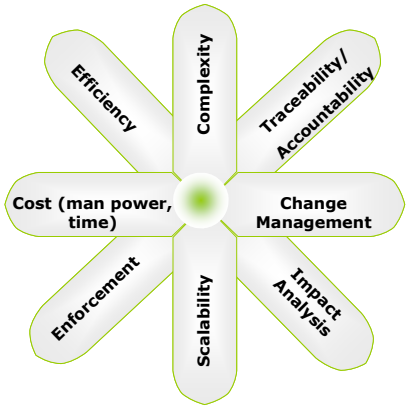

Fig. 3. 8 requirements for assessing an approach to compliance management

- **Change management**: Regulations are by nature subject to change. Regulation evolution should be accompanied by scoping and propagating these changes over the whole domain of jurisdiction of compliance policies. The ability of a framework to do this can make the difference to other approaches and minimize the cost of maintenance of compliance management.

- **Traceability & Accountability**: Policies in a semantic compliance management framework are destined to (i) infer on the state of business processes, (ii) query business processes, (iii) take decisions based upon information policies handled, and (iv) trigger actions on the business and executable process landscape. The chain of decisions and the entities responsible for these decisions have to be documented. As such, a policy-based compliance management framework has to offer functionalities to discover and document which actions were taken, by which resource, for which reasons, and the chain of decisions leading to this action.

- **Complexity**: Complexity is used here in the sense of the complexity of modeling and refers to regulation representation models. A generic compliance management framework should not be custom-tailored to a specific purpose or a specific domain. It has to deal with different degrees of complexity and cover different requirements on the implementation originating from the different supported legislations.

- **Efficiency**: This requirement acts on the policies and the compliance checking algorithms. The question: "Do my policies really constrain my business processes in the way I want them to?" has to be answered. Otherwise, the validity and accuracy of the compliance framework cannot be ensured. The framework must offer functionalities and elements to check and enhance efficiency of designed policies as well as checking and enforcement tools. Without such functionalities, there would be no way the users could make sure they get the most out of their policies and that policies really help processes achieve business goals while not violating regulatory constraints.

- **Cost**: The framework has to be architected and implemented with a fundamental requirement: the overall cost of compliance management (human resources and time) has to be reduced.

- **Enforceability**: A framework that allows defining and managing policies has to provide mechanisms to enforce these policies. Enforcing policies means ensuring business processes are compliant. Enforcement is realized as a human task, because compliance related decisions are taken by people in charge of compliance. The challenge is to (i) formalize decision-making with regard to policy enforcement, (ii) enabling business compliance stakeholders to manage compliance knowledge, and (iii) having tools in the framework capable of interpreting this knowledge for enforcement purposes. This is a step beyond pure compliance checking. Compliance enforcement finds its potentially most attractive realization in highly collaborative scenarios where different business process partners interact, each with its own associated policies.

- **Scalability**: Regulations are very complex specifications and are of a dynamic nature becoming more complex as they evolve. A compliance management framework's efficiency should not suffer from the size of the regulations' space to be managed or from the size of the business processes' scope to cover.

- **Impact Analysis**: Depending on how policies are engineered, some policies may depend on other policies or even be composed of other policies. Introducing changes to policies (either because of changes in regulations or in business goals) or to the compliance framework itself has repercussions on how other policies act and on business processes. Pre-emptive mechanisms (respectively post-change analysis) for predicting (respectively analyzing) the impact of change would add to the efficiency of compliance management. This would provide compliance management stakeholders with ways of tailoring their changes to obtain best

performance from processes. The latter, if allied with versioning functionalities for processes (delivered by the BPM framework) and policies (delivered by the compliance management framework) would complete a lifecycle of compliance management by a controlling phase (see Fig. 7 in section 3.3).

3.2 Types of compliance checking

In this section, we distinguish several ways of viewing the realization of compliance checking. Compliance checking refers to the verification of the status of compliance measures in the enterprise. In the following sub-sections, we introduce different perspectives on compliance checking as shown in Fig. 4.

3.2.1 Design-time/Run-time

We can differentiate between design-time and run-time compliance checking. This is a necessary distinction, because in policy-based compliance checking there is information which is only available at run-time and not at design-time. Thus, policies using this information can only be enacted at run-time like measuring and deciding on service level agreements.

3.2.2 Forward/Backward

There are two ways of realizing compliance checking. One way is to check business process models for compliance. Forward compliance takes place before the execution of the process (design-time) or during execution (run-time). It is a top-down approach to compliance checking. This is a pre-emptive type of compliance checking and can be used in conjunction with business process simulation. It thus requires more reactivity from the business and the process owners than backward compliance checking.

In backward compliance checking, traces left by business processes after execution are used. These traces are often in the form of execution logs. These logs can be processed by business process analysis and mining techniques ([18] and [19]). We note that backward compliance checking is the symmetrical approach to forward compliance checking (bottom-up), since in this case the approach taken is reactive and not pre-emptive. Because it resembles reporting and analysis techniques, backward compliance checking is rather destined to be used for controlling and reengineering purposes.

3.2.3 Active/Passive [a.k.a. Open /Closed]

The distinction can only be asked for forward compliance checking and is easier to see in case of run-time compliance checking. To understand it, we have to ask ourselves how compliance checking can be implemented. Assuming we dispose of a framework for compliance checking, we should ask ourselves whether:

(i) The business process decides when to request the compliance checking components to execute one atomic compliance check and return a decision back, respectively start an action.

(ii) The compliance checking process supervises the compliant execution of the business process or thus does not wait for the business process to ask for an atomic compliance check to be realized, rather deciding itself when to pause the process execution till a decision is made (alternatively compliance checking atomic operations can be fired in parallel to further execution of the process).

In short, passive compliance checking is when the business process execution components control compliance checking operations and active compliance checking is when the compliance checking process controls the execution of the business process.

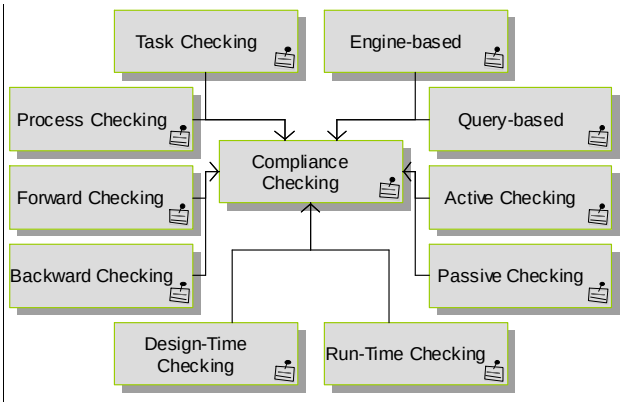

Fig. 4. Categorization of compliance checking

3.2.4 Task Checking/Process Checking [Granularity]

Compliance checking on the level of business process tasks[7] can potentially be different from compliance checking on the business process level, because tasks typically deal with less complexity than business processes themselves. However, in some approaches to BPM, tasks are regarded as being the same as processes by providing the possibility to represent processes embedded in other processes as tasks [4]. So designing a compliance checking framework makes it necessary to clarify such a question, by first knowing what kind of notations will be supported and the meta-model for compliance checking behind it.

3.2.5 Engine/Querying

There are mainly two ways to realize compliance checking. Either the process space can be queried to check for certain rules or policies or a compliance engine that incorporates generic algorithms for compliance checking can be implemented. Both ways make use of an inference engine. In [20] a framework for querying semantic

[7] Tasks are also called activities (BPMN [33] and [34]) or functions (EPC [32]) in existing BPM notations.

business process models using pi-calculus is introduced. These different perspectives can be combined together, i.e. they are not mutually exclusive (e.g. an active design-time checking of EPC-models [32] is possible).

In the next section, we proceed to an initial proposal of a framework for semantic policy-based compliance management for processes.

3.3 Architecture

In the following, we focus on implementing a framework for compliance management. We are not yet at a stage of work that allows us to present a detailed framework. Rather, we define requirements for the framework and justify our choices. We have distinguished five axes upon which we will concentrate our efforts in designing the framework: (i) architecture, (ii) compliance management process, (iii) ontologies, (iv) algorithms, and (v) lifecycle. We have opted for forward compliance checking, design- and run-time checking as well as for passive compliance checking, as aspects that should be supported by the framework in a first stage. These aspects were introduced in section 3.2.

In Fig.5, a high-level view on the architecture of a business process compliance management framework is given. We use Fig. 5 to extract a list of tasks to be realized in order to build the framework. We have identified the following points:

(i) As described in the introduction, regulations need to be formalized in order to be machine-processable. We have to provide mechanisms to formalize regulations as semantic policies.

(ii) These semantic policies have to be modeled into the business processes. In the case of semantic business process management, this means extending the ontology for modeling business processes with an ontology for modeling policies.

(iii) Rules are an intuitive way of implementing policies. Policies have to be transformed into sets of business rules. These business rules can then be integrated into process modeling frameworks and interpreted by an adapted inference engine.

(iv) On a different level, business processes are represented in languages adapted to business process execution. On this level, it is necessary to further transform business rules into operative rules that can be integrated into semantic executable business process models.

(v) A compliance checking engine has to be implemented by building on an inference engine.

(vi) Monitoring components are needed to control the consistency of policies, but also to monitor the checking and enforcement operations on business processes.

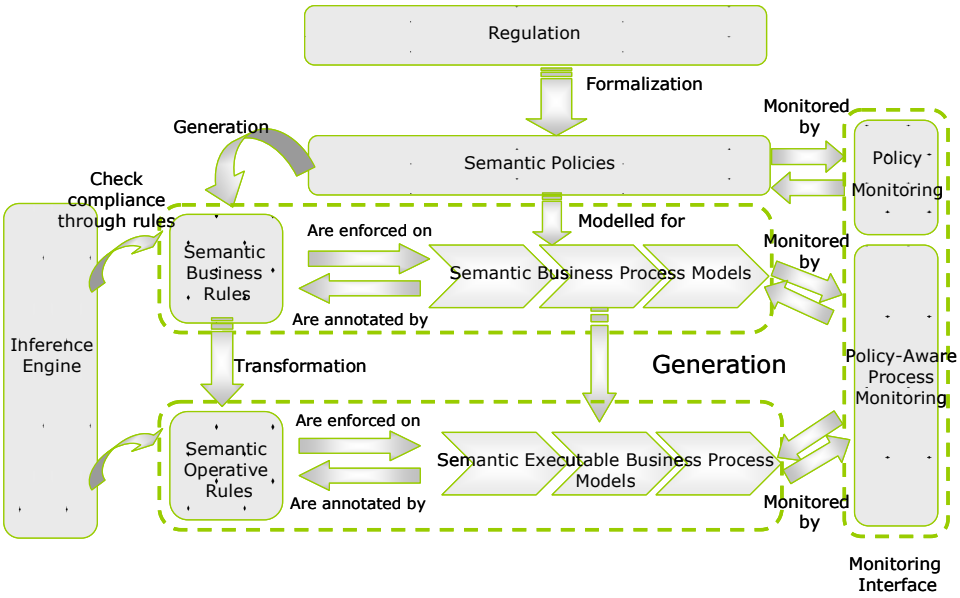

Fig. 5. A high-level architecture for a compliance checking framework

It is evident that in our semantic approach, a good design of ontologies adapted to our needs is necessary. As in [35] and [36], we consider the functional, behavioural, organizational, and informational perspectives for the business process ontology design. In [11], a formal model is proposed for describing business processes taking the previous four dimensions into account (See Fig. 6):

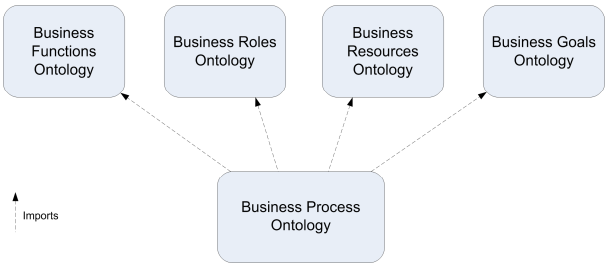

Fig.6. Ontology framework for business processes: functional, organizational, behavioral, and informational perspectives.

While designing the framework, we also have to decide which algorithms will be needed. There is a need for transformations between the various levels of representation of policies (Policies, Business Rules, Operative Rules, Fig. 5). Secondly, there will be the necessity to design compliance checking algorithms to be executed by the semantic compliance checking engine. The semantic compliance checking engine is implemented using an inference engine.

Fig. 7. A proposal for a compliance management lifecycle

We can also see the importance of clarifying the possible uses of the framework by defining compliance management processes, to be supported by the framework and used as an input for the implementation in the user interaction. At this stage, we propose a high-level lifecycle for compliance management (Fig. 7) to be further detailed in future work. First of all, compliance measures have to be defined, which constitute the input for compliance policies. Compliance measures are extracted directly from regulation texts and are organization dependant. After policies have been designed, they have to be implemented by being expressed through business rules for example. Of course, inference can be made on the level of business policies, but it is done at a different level from the implementation. For example, policy inconsistency and conflict discovery or even service negotiations could be done using the policy ontology. Policies have thus to be monitored and controlled (as in [28]), which closes the lifecycle for one compliance management iteration (see section 2.1 and Fig. 3).

In the next section, we have a look at related work dealing with compliance management, semantic business process management, and policy management.

4 Related Work

Compliance management is critical for enterprise governance, as we have shown in the introduction, because business processes take a more and more central place as organizations converge towards process-orientation. There has been ongoing work on semantic compliance management, as shown in [21] and [22], where an approach for semantic compliance management for BPM is presented. However, the approach used concentrates on implementing internal controls. Such an approach is adapted to compliance management but is restrictive because it relies on the necessary definition of risks. Another approach is presented in [29] where the authors introduce the modeling of internal control objectives in business processes as a mean to integrate compliance requirements in business process design. The authors also relate their work to risk analysis and internal control modeling. Policies are meant to be more generic and do not depend on the previous definition of risks in processes. Policies are

meant to be directly extracted from regulations. This introduces a layer between the modeling of regulatory compliance requirements and actual regulatory compliance enforcement. Such a layer would allow for example to exchange policies or discover policy conflicts between business processes existing in different departments or organizations. Moreover, policies can themselves be used to implement internal controls. Policies also allow for profiting from inference mechanisms in order to take decisions through the use of specifically designed policy inference engines such as in [30] and [34].

In [23], a framework is introduced for semantic security management in business processes. However, the presented approach focuses only on security concerns and does not seek to define its own ontologies. It relies on previous work ([30], [31]). In [27] and [24], another approach for business process-based compliance management is presented. It defines an extension for a business process meta-model for regulatory compliance. However, the approach does not incorporate ontologies and thus, does not profit from the power of semantic technologies. In [25] and [26], deontic (obligations and permissions) constraints expressible for business processes are modeled using temporal deontic assignments. The latter can also be used in business process design and in expressing business process contracts.

5 Conclusion and future work

In this paper we have introduced the challenge of regulatory business process compliance management. We also have shown why automated compliance checking becomes a necessity for organizations. We have further seen how the use of policies to model regulations can help implement the latter. We have set as a goal to our work the design of a compliance management framework that is flexible with regard to change in both business processes and regulations. We have defined several requirements for this. We have also distinguished different perspectives on compliance checking. We argued why such a high-level analysis is needed prior to designing a compliance management framework. Finally, we have come up with a high-level architectural description of a framework for business process compliance management.

Working on compliance management places us at the boundary between law and legislations, policies and business rules, risk analysis, ontologies, and business process management. It is an exciting field of research that has a strong relevance for the industry and can have a tangible impact on the way we conduct compliance management today. Upcoming work concerns first of all the design of the policy ontology. We will also get to elaborate an approach for structuring regulations in a form that can be easily represented using the policy ontology. Once we dispose of the ontologies required, the next step would be to implement a first prototype of the architecture presented in section 3.3. To do this, we will need to make and justify technical choices for the elements of the framework, such as ontology languages, inference engines and required transformations and algorithms. We will afterwards

define use case scenarios which we will have to realize using the designed framework. This is intended to validate our efforts.

Acknowledgements. Our research on semantic compliance management is supported by the EU commission within the integrated research project SUPER (http://www.ip-super.org. We would like to thank the EU commission for giving us the opportunity to work on such relevant topics.

References

1. Hartman, T.E.: "The Cost of Being Public in the Era of Sarbanes-Oxley," August 2, 2007
2. Lev, B.: Where have all of Enron's Intangibles gone? Journal of Accounting and Public Policy. 21. pp. 131 – 135, (Summer 2002)
3. Agrawal, R., Johnson, C., Kiernan, J., Leymann, F.: Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. In Proceedings of the 22nd International Conference on Data Engineering (ICDE'06). IEEE Press, 2006
4. Scheer, A.W.: ARIS - Business Process Frameworks. Third edition, Springer, Berlin (1999)
5. Scheer, A.W., Nüttgens, M.: ARIS Architecture and Reference Models for Business Process Management. In: Business Process Management, Lecture Notes in Computer Science, pp. 301-304. Springer Berlin / Heidelberg, January 2000
6. Text sections of the BASEL-II accord, http://www.basel-ii-accord.com/BaselText.htm
7. Chapelle, A., Crama, Y. Hubner, G., Peeters, J.P.: Basel II and Operational Risk: Implications for risk measurement and management in the financial sector. Research series 200405-7, National Bank of Belgium, 2004
8. The ISO 17799 IT security standard: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612.
9. The ISO 27002:2005 IT security standard http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297
10. Congress of the United States. Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act), 2002. Pub. L. No. 107-204, 116 Stat. 745
11. Markovic, I., Pereira, A.C.: Towards a Formal Framework for Reuse in Business Process Modeling. In Workshop on Advances in Semantics for Web services (semantics4ws), in conjunction with BPM '07, Brisbane, Australia, September 2007
12. Schmidt, R., Bartsch, C., Oberhauser, R.: Ontology-based representation of compliance requirements for service processes. In Proceedings of the Workshop on Semantic Business Process and Product Lifecycle Management (SBPM 2007), 2007
13. Zachman Framework, http://www.zifa.com/, http://www.zachmaninternational.com/
14. The Open Group. The Open Group Architectural Framework (TOGAF), http://www.togaf.org/, http://www-128.ibm.com/developerworks/ibm/library/ar-togaf1/
15. Zachman, J. A.: A framework for information systems architecture. IBM systems journal, Volume 26, No. 3, pp 276-292, 1987.
16. Zachman, J. A.: Extending and Formalizing the Framework for Information Systems Architecture. IBM Systems Journal, Volume 31, No. 3, 1992.
17. Uschold, M., King, M., Moralee, S., Zorgios, Y.: The Enterprise Ontology. The Knowledge Engineering Review, 1998. http://www.aiai.ed.ac.uk/project/enterprise/enterprise/ontology.html.
18. Van Dongen, B.F., De Medeiros, A.K.A., Verbeek, H.M.W., Weijters, A.J.M.M., Van der Aalst, W.M.P.: The ProM Framework: A New Era in Process Mining Tool Support. In Applications and Theory of Petri Nets, Lecture Notes in Computer Science. Springer, 2005.

19. Rozinat, A., Van der Aalst, W. M. P.: Decision Mining in ProM. In Business process Management, Lecture Notes in Computer Science, Springer, 2006.
20. Markovic, I., Pereira, A.C., Stojanovic, N.: A Framework for Querying in Business Process Modelling. In Multikonferenz Wirtschaftsinformatik 2008, Munich, 2008.
21. Namiri, K., Stojanovic., N.: Towards Business Level Verification of Cross-Organizational Business Processes. In Workshop on Semantics for Business Process Management (SBPM07), Budva, Montenegro, 2006
22. Namiri, K., Stojanovic., N.: A Formal Approach for Internal Controls Compliance in Business Processes. In 8th Workshop on Business Process Modeling, Development, and Support (BPMDS07), Trondheim, Norway, 2007.
23. Huang, D.: Semantic policy-based security framework for business processes. In Proceedings of the Semantic Web and Policy Workshop. 4th International Semantic Web Conference, 7 November 2005, Galway, Ireland.
24. Karagiannis, D.: A Business process Based Modelling Extension for Regulatory Compliance. In Multikonferenz Wirtschaftsinformatik 2008, Munich, 2008.
25. Goedertier, S., Vanthienen, J.: Designing Compliant Business Processes from Obligations and Permissions, 2nd Workshop on Business Processes Design (BPD'06), 2006.
26. Governatori, G., Milosevic, Z., Sadiq, S.: Compliance checking between business processes and business contracts. In 10th International Enterprise Distributed Object Computing Conference (EDOC 2006). IEEE Press, pp. 221-232, 2006.
27. Karagiannis D., Mylopoulos J., Schwab M.: Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act. In Proceedings of 15th IEEE International Requirements Engineering Conference, New Delhi, 2007.
28. Karagiannis D., Nemetz, M., Schwab M.: Dashboards for Monitoring Compliance to Regulations - A SOX-based Scenario. In Proceedings of IGO'06 - International Conference on Integrating Global Organizations, Siena, 2006.
29. Sadiq S., Governatori G., Namiri K.: Modeling Control Objectives for Business Process Compliance In Proceedings of the 5th International Conference, BPM 2007, Brisbane, Springer, 2007, pp.149-164.
30. Kagal, L.: A Policy-Based Approach to Governing Autonomous Behavior in Distributed Environments. PhD Thesis, Faculty of the Graduate School of the University of Maryland, 2004.
31. Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B., Dean, M.: SWRL: A Semantic Web Rule Language Combining OWL and RuleML. Acknowledged W3C Member Submission. May 21, 2004.
32. Scheer, A.-W.; Thomas, O.; Adam, O.: Process Modeling Using Event-driven Process Chains. In: Dumas, Marlon; van der Aalst, Willibrordus M. P.; ter Hofstede, Arthur H. M. (Hrsg.): Process-Aware Information Systems : Bridging People and Software Through Process Technology, pp. 119-145. Hoboken, New Jersey : Wiley, 2005.
33. OMG: Business Process Modeling Notation, V1.1. OMG specification, formal/2008-01-17, January 2008.
34. White, S.A.: Introduction to BPMN. In BPTrends, July 2004.
35. Uszok, A., Bradshaw, J., Jeffers, R., Suri, N., Hayes, P., Breedy, M., Bunch, L., Johnson, M. Kulkarni, S., Lott, J.: KAoS policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. In Proceedings of POLICY 2003. the IEEE 4th International Workshop on policies for distributed systems and networks. Como, Italy, June 2003.
35. Jablonski, S., Bussler, C.: Workflow Management: Modeling Concepts. *Architecture, and Implementation*. International Thomson Computer Press, London, UK, 1996.
36. Curtis, B., Kellner, M.I., Over, J.: Process Modeling. *Comm. of the ACM*, 35(9):75, September 1992.