Policy-Based Semantic Compliance Checking for Business Process Management

Marwane El Kharbili, Sebastian Stein
IDS Scheer AG, ARIS Research. Altenkesseler Str.
17, D-66115 Saarbrücken, Germany.
{marwane.elkharbili, sebastian.stein}@ids-scheer.com
Elke Pulvermüller
Institute of Computer Science, University of Osnabrück.
Albrechtstr. 28, 49076 Osnabrück, Germany.
elke.pulvermueller@informatik.uni-osnabrueck.de

Abstract: Compliance management, risk analysis, and auditing are disciplines that are critical for large scale distributed enterprise systems. The way these complex systems are developed and deployed makes the management and enforcement of enterprise goals or policies a hard task. This is also true for compliance management of business processes (BPs). Such an observation is emphasized if we give compliance management the scope of the whole enterprise model. In this paper we explain our approach to modeling compliance measures based on policies and present a framework for managing and enforcing compliance policies on enterprise models and BPs. We discuss our ideas in the context of a semantically-enabled environment and discuss why leveraging compliance checking to a semantic level enhances compliance management.

1 Introduction

In past years, an intense public discussion took place dealing with financial scandals happening at major companies and corporations like Enron, WorldCom, Roche, Siemens, and Volkswagen. Based on those events, the importance of compliance management as a critical responsibility at the highest management levels to prevent such scandals has drastically increased. For instance, in 2002 the US government created the "Public Company Accounting Reform and Investor Protection Act" [otUS02], also known as the Sarbanes-Oxley Act, to define mandatory policies for public companies and public accounting companies. Complying with regulations of all sorts is usually needed for purposes ranging from ensuring that specific norms are met (e.g. quality standards such as ISO9000:2005 [fS05]) to proving correct implementation of internal controls imposed by active legislations (e.g. SOX Sec.404 [otUS02]) [KSMP08].
Examples of regulations are the HIPAA[1] (Health sector), FDA regulations[2] (food/drug sector), BASEL-II[3] (Banking sector), ISO27002:2008[4] (IT security) and KonTraG[5] (cor-

[1] Health Insurance Portability and Accountability Act: http://www.hipaa.org/.
[2] US Food and Drug Administration: http://www.fda.gov/opacom/laws/.
[3] Basel II Revised International Capital Framework.
[4] The ISO 27002:2005 IT security standard: http://www.iso.org.
[5] German law for Control and Transparency in the private sector.

porate governance). A given company is likely to be under jurisdiction of several regulations concurrently [KMS07].
The following sections of this paper give a short definition of compliance management and then discuss the problems related in order to grasp the challenges ahead. Section 3 discusses the idea of model-driven compliance checking using policies is and makes a realization proposal. Section 4 introduces a framework for integrated policy-based compliance checking as well as the accompanying ontological framework. Finally, related and future work are outlined before we conclude our contribution.

2 Compliance Management: a definition

Compliance management is a broad term covering all activities and methods to ensure that a company follows all policies required by an external or internal regulation. These regulations are usually described in a natural language document (e.g. as is the case for laws), which can be hardly understood by non-experts of the field the regulation acts on. In the prominent example of the Sarbanes-Oxley Act, if a company follows all guidance defined in such a regulation document, the company is said to be in compliance with the given regulation. Otherwise, the company is said to be violating this regulation.

2.1 Regulatory Compliance

These regulations can be structured and documented in compliance frameworks and complying with the framework is thus regarded as equivalent to complying with the regulation. If no such frameworks exist, then companies have neither guidance nor support for implementing regulations, apart from that of auditors. The examination performed to validate whether a company actually implements a given compliance framework is called audit and the person or organization doing such an audit is called auditor.
Besides legal requirements, in order to use a certain compliance framework, companies often decide to do this for reasons ranging from certification, risk assessment, to the implementation of quality standard implementation, etc. The latter are strategic reasons and do not result from legal pressure exercized by governmental bodies. As an example, practically all companies that reach a certain size decide to endorse quality standards like ISO 9000:2000 [fS05] to publicly demonstrate the company's quality commitment and customer focus.

2.2 Compliance Audits

In order to be successfully audited, a company must in advance ensure that it follows all guidelines defined by the compliance framework. A possible approach for this is to check the degree to which these guidelines are fulfilled by the company's enterprise model. Theoretically, this would have to be done by identifying all relevant aspects of the company's activities on which parts of the compliance Framework apply, and checking this compliance. This task is one of experts who need to either have deep knowledge of the activities, processes, architectures and other enterprise model artifacts of the company (e.g. internal compliance controls), or who are provided tight cooperation with enterprise insiders who

dispose of the necessary knowledge about the activities of the company.
Today, compliance audits are manual and error-prone tasks requiring significant effort. To make the auditing of enterprise models an easier and more efficient task, *automation and full-coverage are key goals*. Moreover, in order to increase quality (in terms of accuracy and credibility of checking reports) and reduce the cost (in terms of human capacities and time) of compliance checking, the idea of using semantic technologies has been proposed [EKSMP08].
Semantic compliance checking relies on a semantically defined compliance framework and uses semantic technologies such as inference engines to evaluate the compliance of a given semantic enterprise model. Our research focuses on *the use of these technologies for designing a policy-based framework for regulatory enterprise compliance management*.

3 Enterprise Regulatory Compliance: The Problem

Compliance frameworks consist of a set of guidance elements and measures that have to be taken in order to follow the latter. These compliance measures are often represented as guidelines, policies or controls, depending on the level of abstraction from the concrete implementation of compliance measures (See figure 1). For instance, the authors of [F.Y07] use the example of an ISO 17799:2002 (IT security standard) access control requirement being further refined into a set of policies. The adherence of a company to these policies has to be evaluated by humans.

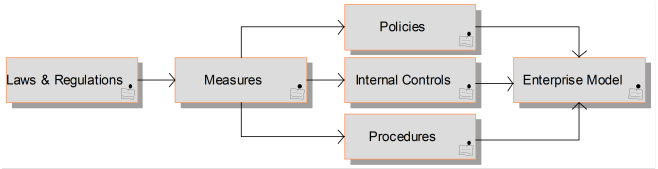

Figure 1: High-Level Compliance Model

3.1 Example: Segregation of Duty (SoD)

The Sarbanes-Oxley Act defines the rule that a financial auditor of a company is not allowed to also be involved in the bookkeeping or accounting of the audited company ([otUS02], Sec. 201 (g) (1)). Such a rule is part of a more complex set of rules specifying which concrete roles/responsibilities can be concurrently carried out by an individual. This set of rule is regrouped under the term SSegregation of Duty (SoD)ppolicy. In concrete cases, SoD policies are two-dimensional matrixes of available roles where SoD violations can be visualized in the cells where two roles cross each other. This is shown in the following simple example in figure 2 by specifying which tasks can be concurrently realized by the same individual.

In this example, the auditor must examine who did the bookkeeping and the financial audit and that both roles are not shared by one person or organization. Given the fact that a compliance framework usually consists of many policies, it is a significant effort for an

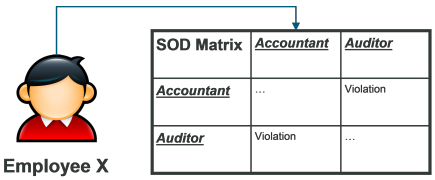

Figure 2: Segregation of Duty (SOD) policy example

auditor to check all of them and for all concerned employees. Therefore, an auditor picks (based on experience or randomly) a set of business artifacts upon which policies have to be checked. This helps to reduce the auditing effort, but this strategy cannot be applied by a company to ensure compliance before the actual audit takes place, neither does it guarantee the benefits of being a highly compliant company with target regulations (i.e. this is particularly relevant in case of quality standards audit).
The consequences of a failed audit can be significant. For example, if a public company finds itself forced to delay its annual balance because of a failed financial audit, it might loose significant market capitalization (e.g. falling stock price resulting from loss of confidence in the market). Consequently, complying with all policies defined by a specific compliance framework becomes a precondition for realistic preparation to an audit. One of the challenges identified here is: how to structure compliance and how to model it?

3.2 Enterprise Compliance Management and Enterprise Models

Compliance is all about control, and it is hard to control what is not thoroughly known. Companies create enterprise models to represent their structure and dynamics. Various guidelines to structure such a model exist like the Zachman [JAZ92], the TOGAF [Gro] or ARIS [Sch00] frameworks. An enterprise model is used to document the as-is reality of a company as well as a planning tool for to-be scenarios. Another dimension in enterprise models is capture full semantics of the latter and thus allowing for machine processability of the information available about these models. There are various research efforts made to formalize the underlying meta-models of enterprise models using Ontologies [HLD+05, UKMZ98]. Enterprise models span the whole vertical structure of a company and contain among others BP models and internal governance policies.
On the other hand, regulations, which guide the development of compliance frameworks, are usually available as text documents, often requiring juristic skills to interpret them correctly. Not surprisingly, checking a given enterprise model for compliance is therefore a manual task carried out by certified domain experts. Furthermore, efficient compliance management requires good knowledge of the enterprise model of a company by the auditors, and a good knowledge of the compliance framework by the management. This makes close collaboration of auditors with management boards a necessity. The challenge of automated compliance checking can be seen as *extending an enterprise model* to include aspects defined by the compliance framework and *enabling the needed automation in checking an enterprise model against the policies* defined in a compliance framework.
We argue that *measures defined in order to ensure regulatory compliance can be repre-*

sented using policies (See figure 1). Thus, enforcing these policies guarantees a state of compliance. Putting policies to use for this purpose allows profiting from policy management formalisms and frameworks. We also argue that making use of semantic technologies for representing compliance policies is necessary to deal with semantically lifted process models. It also *helps making compliance checking more precise by allowing to model compliance policies at higher abstraction levels in order to cope with the ambiguity inherent to regulations*.

4 Semantic Policy-Based Compliance Checking

4.1 Formal, Declarative, Semantic & Domain-Dependent Policies

Policies have to be structured and expressed using formal means making their automatic processing possible. The authors of [LGRM+08] see modeling compliance constraints in declarative fashion, while respecting a trade-off between expressiveness of the formal language used and the cost of inference and analysis. Declarative languages are supported as the preferred approach to modeling compliance as a number of works show [LGRM+08, IWH, ZM06, GG06]. This has the advantage of separating between compliance models and targeted enterprise models. In comparison to approaches such as the one presented in [DF06], it also has the advantage of better scaling with regulation change and complexity of the targeted enterprise models.

Policies can also be expressed using formalisms such as rules. Rules are one classical and very intuitive way of expressing/implementing policies. In [OMG], the SBVR[6] standard is defined for expressing rules and vocabularies on a business level. While providing a natural-language-like syntax that is very easy to use for business users, an underlying formalization of used rule constructs is provided. However, rule interpretation and execution is not enabled because of a missing mapping to an executable rules language. The PRR[7] [OMG07] standard could fill this gap as it is designed to transport production rule logic and a mapping to SBVR would create the link for rules from the business level to a rule engine (execution) level.

Enterprise models describe architectures, processes and architectures at different degrees of detail and under various perspectives. They usually deal with high heterogeneity on both business and technical levels[JAZ92, Sch00] (strategic, tactical, business, operational and technical levels as distinguished in [vl01]. Ontologies allow *Achieving interoperability between multiple representations of reality[...]and between such representations and reality, namely human users and their perception of reality.* [Hep07]. As compliance is a vertical concern, a compliance framework needs to handle the different perspectives on the various layers. These layers and perspectives can be integrated on a semantic level giving meaning to the relationships between them. The work realized in the SUPER[8] Research project seek to build a stack of ontologies for BPM doing just this. In [Jab96, Cur92], the functional, behavioral, organizational, and informational perspectives are considered for the BP ontology. In [IM07], a formal model is proposed for describing BPs taking the previous four dimensions into account. A compliance framework should then support

[6] Semantics of Business Vocabulary and Rules

[7] Production Rule representation

[8] Semantics Used for Process management within and between EnteRprises. www.ip-super.org.

handling this integrated these ontologies and support automated checking/enforcement of policies on instances of these ontologies.

4.2 An Approach to Compliance Management

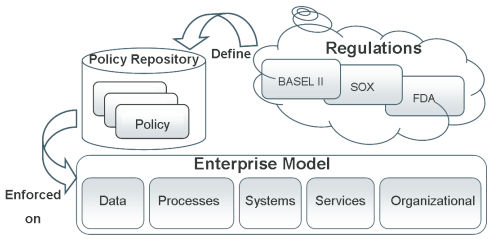

Figure 3: An approach for compliance formalization using policies

Our proposal for handling the aspects we just cited is *semantic compliance checking (SCC)*. SCC extends enterprise models semantically to integrate semantically described policies with semantic enterprise models. The initial Input are, as is the case for auditors, the actual regulations, laws or norms that define the policies to be compliant with. These can be structured and represented using dedicated domain policy ontologies (e.g. IT security, food regulation etc.). These policies are then made available in a policy repository for integration into enterprise models. A compliance engine specifically implemented on the basis of an inference engine for the policy ontology language embodies the necessary compliance checking algorithms. This approach is shown in figure 3. Existing works follow a aimilar idea, as in [SN07, NS07b], although concentrating on risk management approaches to compliance checking. Other works already started formalizing regulations such as the Sarbanes-Oxley-Act [KMS07] and BASEL II [RF06]. Due to the organization or regulations in separate domains of enactability, it is possible to separate policy ontologies per domain, making an additional level or *super-policies* ontolgy necessary in order to link domain policy ontologies together. This allows e.g. combining policies and enacting them concurrently on the same enterprise model.

5 An Architecture for Compliance Management

5.1 Enterprise Models: A Layered View

An enterprise's structure can be seen as the set of layers distinguished in 4. On the top layers are business goals which are fulfilled by defining corporate strategies. These strategies are supported by policies and governance guidelines. Policies constrain and control business artifacts: BPs, business rules, business data (vocabularies), etc. On an inferior layer are operational artifacts such as operational rules and executable processes. The lowest layer in this view contains the applications, components, systems and deployment environments that host the concrete carriage of IT activities.

This view of the enterprise can be mapped to a paradigm that we call Decision-Action-Information (DAI) as shown in 4. In this paradigm, the enterprise is seen as composed of

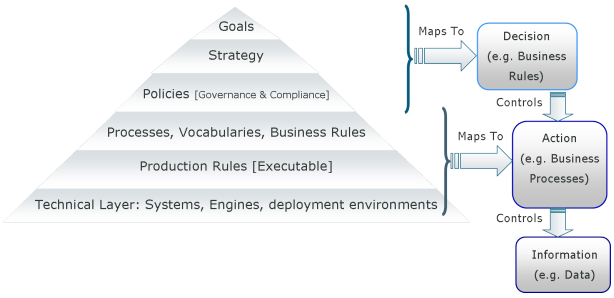

Figure 4: A layered view on the enterprise for compliance

three basic classes of artifacts. The decision class contains all artifacts supporting decision management such as business rules. The action class contains logical and operational artifacts that actually carry out business activities. Finally, the Information class contains all data artifacts such as execution logs or database tables, on the basis of which decision are partly taken and which are needed by action class artifacts in order to realize their functionality. Our work hypothesis is that compliance is defined for action artifacts and needs to be modelled as decision class artifacts.

5.2 A Framework for Compliance Management

In the following, we focus on designing a framework for compliance management shown in figure 5. This framework does not yet define a detailed technical architecture, it rather defines requirements. We have distinguished five axes on which efforts will concentrate: (i) architecture, (ii) compliance management process, (iii) ontologies, (iv) compliance checking algorithms, and (v) policy management lifecycle. The following points have been retained:

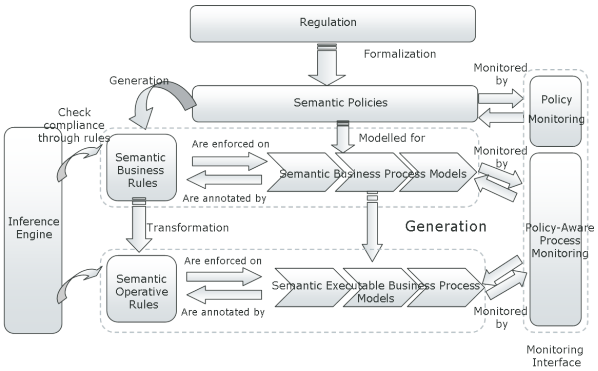

Figure 5: An Architecture for a compliance checking framework

- regulations need to be formalized in order to be machine-processable. We have to

provide mechanisms to structure and then formalize regulations as semantic policies.

- semantic policies have to be modelled into BPs. In the case of semantic business process management (SBPM), this means extending the ontology for modeling BPs with an ontology for modeling policies.
- Rules are an intuitive way of implementing policies. Policies have to be transformed into sets of semantic business rules. It implies defining a business rules ontology and selecting an ontology language supporting expressing rules. No assumptions about the expressiveness and the kind of logic supported by this rule ontology language have been made yet. These business rules can then be integrated into process modeling frameworks and interpreted by an adapted inference engine.
- BPs are represented in languages adapted to BP execution. On this level, it is necessary to further transform business rules into operative rules that can be integrated into semantic executable BP models.
- A compliance checking engine has to be implemented by building on an inference engine. This compliance checking engine implements generic compliance checking algorithms.
- Monitoring components are needed to control the consistency of policies, but also to monitor the checking and enforcement operations on BPs.

Three main layers have been identified and need to be regarded separately. The policy layer is the management layer where policies are expressed, and functionalities such as conflict resolution, speech acts, delegation, policy priorities, meta-policies and the definition of jurisdictions are available. Policy consistency checks also take place on this layer. The second layer contains design-time artifacts such as BP models and business rules. Just as BP models need to be transformed into executable process models that can be run on several execution engines, business rules need to be transformed into operative rules which can be run on the same layer as BP execution engines. The prefix ßemanticmmeans that policies, BP models, executable BP models, business rules and operational rules are all defined using dedicated ontologies.
Additionally to these layers, there are two vertical components: the monitoring components and the inference engine. Monitoring is needed both for the operations taken on policy models and for monitoring design-time and run-time decisions taken by policies which closes the lifecycle for one compliance management iteration.. This requirement has also been identified in [KD06]. The inference engine operates on both business rules and operational rules (which implement the decision-making logic behind policies) in order to check for regulation policy violation. The policy layer disposes of its own engine for inferring on policy management aspects such as inconsistency or conflict detection.

This framework requires the definition of a set of transformations. Figure 6 shows how policy layers map to semantic layers. The semantic policy layer contains ontologies for definition and management of policies as well as domain policy layers. A first transformation is needed in order to generate business rule models out of the policy definitions. A

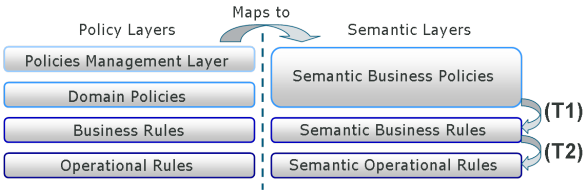

Figure 6: Policy layers and transformations in the framework

second transformation is needed in order to generate operational rule models out of business rules models. Our goal is to define languages (in the form of ontologies) for each of these layers and to complete these with generic transformations between the ontologies. We are currently concentrating on the definition of an ontology for policies and rules. Future work will include the definition of mappings to the SBVR [OMG] and PRR [OMG07] standards.

Figure 7: Managing policies

A lifecycle needs to be defined for the management of semantic policies. Figure 7 makes use of the components identified in the architecture for this lifecycle. After being defined (as a policy ontology instance), a policy must be verified for formal consistency and conflicts with other ontologies. The next steps will then be to generate design-level and execution-level models of these policies and to enforce them on BPs. Furthermore, analyzing the execution of policies and the decisions takes by the latter completes the lifecycle and provides insights into how tight do the designed policies match the initial regulations. The analysis phase outputs also serve as audit artifacts that can show that the right policies have been defined and that these are working correctly.

6 An Ontology for Policies and Rules

The business policy and Rule ontology (BPRO) we introduce has been modelled to fulfill the requirements we already identified. In the following, we will shortly introduce its main concepts and relationships. Because of space restrictions, the ontology components won't be introduced in detail (i.e. information to cardinalities and examples are not included).

Figure 8 shows the core policy ontology. The central concept is the policy concept. A policy is a meta-policy if it is enacted on other policies. A policy belongs to a strategy and is part of the implementation of one or many regulations. A policy fulfills a business goal. A constraint is one kind of policy, next to Decision, functional and core policies. A constraint policy decides on how to constrain a resource in showing some behavior. It delivers one or many of several discrete allowed business artifact behaviors/states and does not provide a binary yes/no answer as a decision policy does. A core policy is a policy which takes no decision that has to be enforced on business artifacts, it can only be invoked by

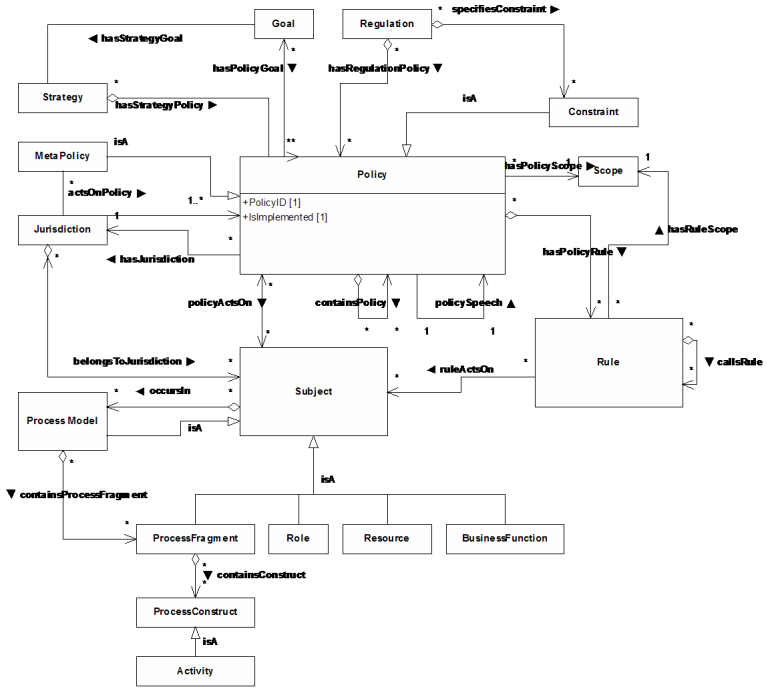

Figure 8: Policy Ontology

other policies and delivers intermediary decisions. A functional policy applies for business functions that are able to execute differently depending on the parameters given to them. A functional policy decides on which concrete action these business function as can take by setting these parameters.

A policy has a subject, which is the entity(ies) on which it can apply. This subject can be a process model for example or any business artifact part of the enterprise model (e.g. role, resource, business function etc.). A process is composed of process fragments and the latter are composed of process constructs such as activities. The concepts related to BP modeling have to be mapped to the used BPM ontologies.

A policy has a jurisdiction and a scope. A jurisdiction is the domain in which a policy has the right to take decisions. Outside its jurisdiction, a policy cannot take any decisions, cannot be solicited, and cannot communicate with other policies about subjects not belonging to its jurisdiction. A Jurisdiction is a set of subjects. These sets of subjects can be defined in a declarative way, such as using assertions on properties of subjects: **all roles of type==[engineer | manager] where role.budget>= 1000 units**. We do not take into account jurisdiction management (which would require a dedicated algebra) in order to define these inter-policy relations unambiguously. Scopes are different from a jurisdiction in that scopes are always strictly included in jurisdictions and define the set of subjects inside a given jurisdiction upon which a policy can take a decision. Scopes introduce additional flexibility in managing policies, by allowing to mmoveä policy's scope inside a

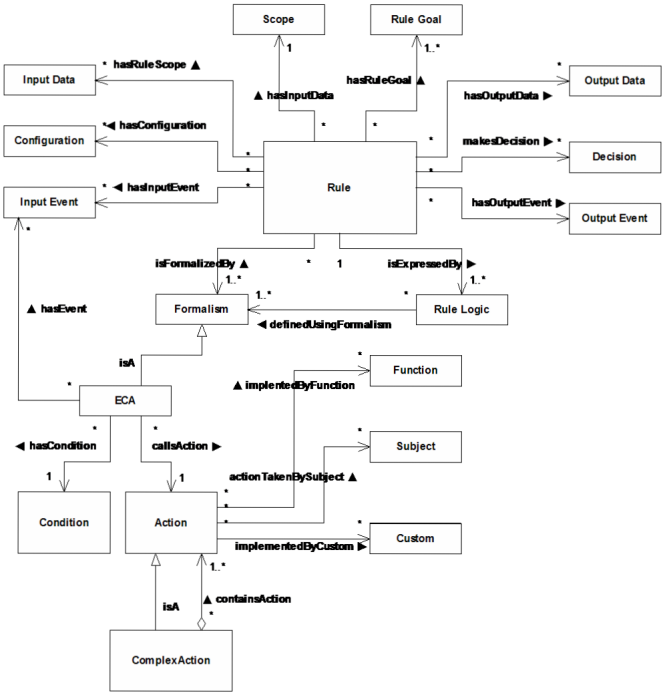

Figure 9: Rule Ontology

given jurisdiction.
A rule belongs to one or many policies. That means rules can be composed in order to implement a certain policy. A rule is also attached to a business goal and has a scope. A rule has input and output data it processes and an input and output event. Input events can trigger the execution of a rule and output events are generated by a rule to trigger other rules or actions. A rule has configuration data which makes a rule able to execute different logic depending on its configuration. A rule makes a decision.
A rule contains rule logic which is expressed in a certain formalism. Formalisms are many and in the figure above, the Event-Condition-Action (ECA) formalism has been used as an example. An ECA rule has a condition and an action which can be a complex expression of actions. It is also triggered by one of the input events of the rule. The action taken by the ECA rule is done on a subject.

7 Related Work

There has been ongoing work on semantic compliance management, as shown in [NS07a], 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 [SN07] where the authors introduce the

modeling of internal control objectives in BPs as a mean to integrate compliance requirements in BP design. The authors also relate their work to risk analysis and internal control modeling. Policies are meant to be generic and do not depend on a previous definition of risks in processes.
In our approach, policies are meant to be directly extracted from regulations, either in automated fahion, by relying on natural language processing techniques, or semi-automated fashion, by generating policy templates out of regulatory documents for the policy expert to complete. 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 BPs 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 [Kag04].
In [Hua05], a framework is introduced for semantic security management in BPs. However, the presented approach focuses only on security concerns and does not seek to define its own ontologies. It relies on previous work ([Kag04, ea04]). In [KMS07] and [Kar], another approach for BP compliance management is presented. It defines an extension for a BP meta-model for regulatory compliance. However, the approach does not incorporate ontologies and thus, does not profit from the power of semantic technologies. In [GV06] and [GG06], deontic (obligations and permissions) constraints expressible for BPs are modelled using temporal deontic assignments. The latter can also be used in BP design and in expressing BP contracts.

8 Conclusion and Future Work

In this paper we have thoroughly introduced the business problem of compliance checking and motivated the need for a comprehensive compliance management framework. We proposed and justified the use of policies for this purpose, which decision is also supported by existing works. Enterprise models are defined semantically and enriched with compliance measures modelled as elements of a policy ontology. This requires an integration of enterprise models and compliance management models. Specifically implemented inference engines can be used to reason over the resulting models and decide on or enforce compliance. An architecture has been presented in order to illustrate our approach. The different layers, components and interactions between these components as well as necessary model transformations were introduced. The first steps towards implementing this framework have been taken and an ontology proposed. While we go further in realizing a reference implementation of the proposed architecture, new requirements will appear and can push us to slightly modify the architecture. As a next step, we will design tools to allow editing and building compliance policy ontologies. We also will define and implement the necessary ontology transformations discussed above. As a proof-of-concept, we will seek to define realistic use cases for a specific domain (e.g. quality management) and shocase the use of the compliance framework. Ultimately, the goal of this work is to showcase how using semantics, policy management and rule management can make

compliance checking automatable[9].

References

[Cur92] Kellner M.I. Over J. Curtis, B. Process Modeling. Comm. of the ACM, September 1992. 35(9):75.

[DF06] Wilhelm Rossak Daniel Foetsch, Elke Pulvermueller. Modeling and Verifying Workflow-based Regulations. In *Proceedings of the international workshop on regulations modeling and their validation and verification. REMO2V06.*, pages 825–830. CEUR-WS.org/vol-241, Luxemburg, June 2006.

[ea04] Tabet S. et al. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. W3C Member Submission 21, May 2004 2004.

[EKSMP08] Marwane El Kharbili, Sebastian Stein, Ivan Markovic, and Elke Pulvermüller. Towards Policy-Powered Semantic Enterprise Compliance Management – Discussion Paper. In *3rd International Workshop on Semantic Business Process Management (SBPM)*, CEUR Workshop Proceedings, Tenerife, Spain, June 2 2008.

[fS05] ISO International Organization for Standardization. ISO9000:2005 - Quality management systems, Fundamentals and vocabulary., 20.09.2005 2005.

[F.Y07] N. Parameswaran & P. Ray F.Yip. Rules and Ontology in Compliance Management. In *Proceedings of the 11th IEEE International Enterprise Distributed Object Computing Conference*, number 1541-7719, page 435, Washington, DC, USA, 2007. Washington, DC, USA, IEEE Computer Society.

[GG06] Shazia Sadiq Guido Governatori, Zoran Milosevic. Compliance checking between business processes and business contracts,. In *Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06)*, pages pp. 221–232, 2006.

[Gro] The Open Group. The Open Group Architectural Framework (TOGAF).

[GV06] Stijn Goedertier and Jan Vanthienen. *Designing Compliant Business Processes with Obligations and Permissions*, volume 4103 of *LNCS*, chapter BPM 2006 Workshops, pages 5–14. Springer Verlag, 2006.

[Hep07] Martin Hepp. Ontologies: State of the art, business potential, and grand challenges. In Martin Hepp, Pieter De Leenheer, Aldo de Moor, and York Sure, editors, *Ontology Management: Semantic Web, Semantic Web Services, and Business Application*, pages 3–22. Springer, 2007.

[HLD+05] M. Hepp, F. Leymann, J. Domingue, A. Wahler, and D. Fensel. Semantic Business Process Management: A Vision Towards Using Semantic Web Services for Business Process Management. In Francis C. M. Lau, Hui Lei, Xiaofeng Meng, and Min Wang, editors, *ICEBE*, pages 535–540. IEEE Computer Society, 2005.

[Hua05] Dong Huang. Semantic policy-based security framework for business processes. Proceedings of the Semantic Web and Policy Workshop - csee.umbc.edu, November 2005. 4th International Semantic Web Conference, 7 November 2005, Galway, Ireland.

[9]**Acknowledgements: We thank the EU commission for supporting our research within the SUPER project (*www.ip-super.org*).**

[IM07] Alessandro Costa Pereira Ivan Markovic. Towards a Formal Framework for Reuse in Business Process Modeling. Workshop on Advances in Semantics for Web services (semantics4ws), in conjunction with BPM '07,, September 2007 2007. Brisbane, Australia, September 2007.

[IWH] Guido Governatori Ingo Weber and Joerg Hoffmann. Compliance Checking for Process Repositories. In Dr Michael zur Muehlen Dr Shazia Sadiq, Dr Marta Indulska, editor, *Proceedings of the Workshop on the Impact of Governance, Risk, and Compliance on Information Systems (GRCIS)*. Montpellier, France, June 2008.

[Jab96] Bussler C Jablonski, S. *Workflow Management: Modeling Concepts. Architecture, and Implementation.* International Thomson Computer Press., London, UK., 1996.

[JAZ92] J. F. Sowa J. A. Zachman. Extending and Formalizing the Framework for Information Systems Architecture. *IBM Systems Journal*, Volume 31, No. 3,, 1992.

[Kag04] Lalana Kagal. *A Policy-Based Approach to Governing Autonomous Behavior in Distributed Environments.* Phd thesis, Faculty of the Graduate School of the University of Maryland, 2004.

[Kar] D. Karagiannis. A Business process Based Modelling Extension for Regulatory Compliance. In Multikonferenz Wirtschaftsinformatik 2008, Munich, 2008.

[KD06] M. Schwab M.: In Karagiannis D., Nemetz. Dashboards for Monitoring Compliance to Regulations - A SOX-based Scenario. In *Proceedings of IGO'06 - International Conference on Integrating Global Organizations. Siena, 2006.*, 2006.

[KMS07] Dimitris Karagiannis, John Mylopoulos, and Margit Schwab. Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act. In *Requirements Engineering Conference, 2007. RE '07. 15th IEEE International*, pages 315–321, 2007.

[KSMP08] M. El Kharbili, S. Stein, I. Markovic, and E. Pulvermüller. Towards a Framework for Semantic Business Process Compliance Management. In S. Sadiq, M. Indulska, and M. zur Muehlen, editors, *GRCIS Workshop - CAISE Conference*, 2008.

[LGRM+08] Linh Thao Ly, Kevin Göser, Stefanie Rinderle-Ma, , and Peter Dadam. Compliance of Semantic Constraints A Requirements Analysis for Process Management Systems. In Sadiq S., Indulska M., and zur Muehlen M., editors, *Proceedings of the GRCIS08: International Workshop on Governance, Risk and Compliance - Applications in Information Systems.*, June 2008.

[NS07a] Kioumars Namiri and Nenad Stojanovic. A Formal Approach for Internal Controls Compliance in Business Processes. In *8th Workshop on Business Process Modeling, Development, and Support (BPMDS07)*, page 9, Trondheim, Norway, 2007. BPMDS07.

[NS07b] Kioumars Namiri and Nenad Stojanovic. *Using Control Patterns in Business Processes Compliance*, volume 4832/2007, pages 178–190. 2007.

[OMG] OMG. OMG Business Modeling Specifications - Semantics of Business Vocabulary and Rules.

[OMG07] OMG. Production Rule Representation (PRR) - Beta - OMG adopted specification. http://www.omg.org/docs/dtc/07-11-04.pdf, November 2007.

[otUS02] Congress of the United States. Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act). Pub. L. No. 107-204, 116 Stat. 745, 2002.

[RF06] Andre Rifaut and Christophe Feltus. Improving Operational Risk Management Systems by formalizing the BASEL II Regulation with Goal Models and the ISO/IEC 15504 Approach. In *Proceedings of the REMO2V06*, page 831, 2006.

[Sch00] August-Wilhelm Scheer. *ARIS - Business Process Frameworks*. Springer, 3rd ed. edition, April 2000.

[SN07] Governatori G. Sadiq, S. and K. Namiri. *Modeling Control Objectives for Business Process Compliance*, pages 149–164. Lecture Notes in Computer Science. Springer, 2007.

[UKMZ98] Mike Uschold, Martin King, Stuart Moralee, and Yannis Zorgios. The Enterprise Ontology. *The Knowledge Engineering Review*, 13, 1998. http://www.aiai.ed.ac.uk/project/enterprise/enterprise/ontology.html.

[vl01] A. van lamsweerde. Goal-Oriented Requirements Engineering: A guided tour. In *Invited minitutorial, proceedings of the RE01*, pages 249–263. International Joint Conference on Requirements Engineering, Toronto IEEE., August 2001.

[ZM06] M. Orlowska Z. Milosevic, S. Sadiq. Translating business contract into compliant business processes. In *Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06)*, pages pp. 211–220, 2006.