A decision-support system for IS compliance management

Lotfi Hussami[1,1,]
[1] HEC – Lausanne, Institute of Information Systems
lotfi.hussami@unil.ch

Abstract. IS compliance in nowadays a necessity for organizations in terms of reputation, profitability and performance. The complex nature of the regulations and their big number make it difficult to assess the impacted regions of an enterprise by a given regulation. In this paper, we propose an ontology-based architecture that support IS compliance management by formally computing the gap between the regulations and the IS. We go also beyond the process view of compliance and propose the use of an Enterprise model in order to treat the compliance with a more holistic view of the organization.

Keywords: compliance, legal ontologies, requirements elicitation, requirements enforcement, Model Driven Architecture, Enterprise Model, decision-support system.

1 Introduction

In the last few years, *compliance* with regulations (laws, standards, internal policies, etc…) has become a new and important aspect of an IS, very similarly to how the *security* concept before evolved from a quality to become nowadays a necessity in almost any IS. Being compliant, in our view, means not only to adhere to the law, but being able to prove it as well. With a continuous flow or regulations that are ambiguous, complex, and potentially incoherent (since coming from different sources), introducing compliance requirements and merging them with others IS requirements is a hard task that is -depending on the internal organization- experienced by either system designers, compliance officers, or requirements engineers. Indeed, currently the approach is mainly *reactive* "with one-off, best-of-breed solutions that address today's immediate need"[1], which makes the compliance viewed as pure costs[2]. We identify two concerned levels with this issue: the legal requirements elicitations and their enforcement; and two problems that are associated with these two levels: traceability (ability to draw and compute the paths showing the regulations impact on the system, and then the path from the requirement to the IS components), and flexibility (the IS ability to adapt to regulations). We believe that if the compliance is considered currently as a burden and is badly respected it's because there is no artifact that can provide a proactive, sustainable and *holistic* solution[3] ensuring the *flexibility* and *traceability* features mentioned above. Such a solution

[1] Supervised by Prof. Yves Pigneur (yves.pigneur@unil.ch).

would not only facilitate the overall compliance management, but improve as well the business performance (e.g. by improvement of the reporting tools) and the transparence of the alignment between the legal/business requirements and the IS. Building on that, the research question we want to address is: **How to help for the IS compliance management through a decision support system that would provide traceability and flexibility?** In this paper we propose an architecture for a decision support system that should be able to make a gap analysis between a set of regulations and the current set of specifications, and detect the impacted zones of an architecture by a given regulation. The second module would allow generating directly -based on the gap analysis and the user decision- the pieces of software to be put in place; this would answer the flexibility requirement. The main novelties in our proposition are the use of legal ontology and Enterprise model ontology in an integrated manner in order to address the research question.

We adopted the Hevner design science framework [4] to conduct our research. We started by making a broad literature review trying to detect *relevant* problems that were not addressed, driven by the intuition that a more holistic [3] and formal approach for compliance is needed. In the next section we will go through the state of art in the IS compliance field. Then we will show the state of our research, i.e. the work already done and what is our proposition. Finally we will present more concretely our research objectives, and then and we summarize our contributions in a conclusion.

2 State of art

We have selected sources both from the academic journals and from research groups like Forrester Inc. and Gartner Inc. Several fields are touched by the compliance problem, mainly these three domains: requirements engineering, regulation formalization and compliance checking.

Regulation formalization is a first and crucial step in any compliance management approach for IS and it is mentioned by [5] and [6] as a task to achieve in the beginning of the compliance management activity. The regulation formalization has often been addressed as a sub-task in the design of a system that deals with compliance. For instance [7] proposed a law formalization as hierarchical taxonomy of regulations guise XML structure, coupled with a reasoner as a compliance-checking assistant. Another effort is in the frame of the REALM project, the approach given by [8][9] proposes a "*Concept Model that captures the concepts and relationships occurring in a regulatory domain*", and proposes a set of generic concepts to be extended depending on the case to describe. We extended our literature review to the efforts that are focused only in formalizing the law independently from the application domain, and we found intensive work that has been already been conducted to build legal ontologies based on OWL like the Core Legal Ontology (built on DOLCE+)[10], and more recently the Legal Knowledge Interchange Format (LKIF) in the frame of the Estrella project[11]. LKIF provides and can manipulate concepts such that *permission*, *obligation* and *prohibition*, and the semantic relationships between them. Legal ontologies have a considerable potential in a

compliance IS, since legal knowledge management needs an approach that goes beyond solving classical ambiguity or contradictions handling; it opens the door for the use of legal reasoning that have the potential to provide specific legal use cases; Gangemi [12] proposes a list of them, e.g. conformity checking and Legal advice

Compliance checking of an organization is obviously a major activity in the compliance management process. The TUDOR center proposed a process assessment framework based on the ISO 15504 standard for process assessment, under the assumption that this standard has capabilities that goes beyond the IT domain [13]. The authors propose to use a Goal-Oriented Requirement Engineering (GORE) approach to obtain the necessary requirements and ease the checking task we have to do when conducting an assessment that will measure the process capability (compliance level). Still at the process level but going at a finer granularity, some researchers considered the conformity checking task at the level of the executions paths. [14] considered the problem of checking the conformity of a business process execution against the terms of a contract, by adopting for both a common event-based formalism. [15] considered the problem of checking the conformity of the process models rather than the instances, by testing these models against a set of business rules. Note that this practice provides as well assistance for business process compliant design.

Compliance monitoring is performed during the execution, and furthermore a reaction mechanism is defined to face non-conformity. [16] from SAP proposed the implementation of the Internal Control process imposed by the Sarbanes-Oxley Act as semantic layer above business processes. A related work is [17] from IBM, which proposes to view the internal control processes as in an organization as "a set of workflows, each containing required control activities" to obtain business process modeling, rules enforcement, and auditing.

Risk and Business Process design: [16] (mentioned above) considers the risk assessment task when building the semantic mirror. [18] then proposes an approach to design and model business processes by considering the risks they are exposed too. For this purpose they propose a risk taxonomy, a taxonomy of the business process elements exposed to risk, and a set of risk handling strategies.

Semantic technologies for compliance assistance: [5] claims that since the information is the cornerstone of any effective risk & compliance process, the compliance applications need a more powerful technology to deal with the information complexity than a syntactical approach that relies on keywords and unstructured textual descriptions, and so they argue for the use of semantic technologies (ontologies).

By measuring the state of art with our research question and problem formulation, we noticed that mainly the efforts were concentrated on the requirements engineering, business process design and checking, and regulations formulation. In the other hand, people worked on the legal formalization, but with a broader vision than specifically the IS compliance issue. We are not aware of efforts to treat the compliance in an integrated way combining all the separate works made, so we share [6] view claiming that “regulations are destined to be enacted on the complete enterprise model, not only on business processes”.

3 State of our research

Previous work

As already mentioned, we started our work by a broad exploration of the state of art in what is related to compliance in order to analyze and understand the problem. We augmented that with an experience in industry through an internship in a prominent Swiss financial institution. The results are presented in a first paper we wrote [19] where we presented two frameworks. First we followed and supported the idea that compliance should not be treated as a set of independent projects, and so we proposed a holistic process interacting with the Governance and Risk Management within an organization and working on aligning them. The second proposition was a framework recalling the strategic alignment model of Henderson & Venkatraman, in which we consider the compliance problem as an alignment problem between different domains: the regulations, the internal policies, the available IT compliance artifacts, and the IT compliance requirements. Each of these domains has to be aligned with another one depending on the situation.

Current state

In this paper we propose an architecture for a decision support system that will helps in the requirements elicitations and their enforcement. When a new regulation comes, typical questions that arise to an IT compliance officer are:

- What parts of my architecture are impacted by this regulation?
- Is this regulation contradicting/ overlapping with another one I'm already compliant with?
- What do I need to change in order to be compliant with this regulation?
- Am I already compliant with this regulation?
- Could this regulation be interpreted in a way that would be more convenient for me?

Requirements elicitations

The idea is then to compare and analyze two representations: a model of the regulations, and a model representing the current state within the organization (Fig.1). Previous works we mentioned in the state of art already explored this idea at the process level. However -as mentioned above- we claim that the process perspective, although necessary, is not sufficient since having compliant individual processes doesn't mean that the set of all the processes is also compliant. Regulations also could involve directives about reports formats for instance, which would not really fit in a representation based on processes. By going further in the abstraction, and driven by our concern about a more integrated view of the compliance, what we would like is rather confront the following two models: the regulations model and the whole enterprise model; this will enable us to perform a gap analysis between the current

enterprise model and the ideal ideally compliant enterprise model, the whole in a formal way. A formalism transversal to the organization is then needed to express and establish the relationships between the different layers of the enterprise architecture. This formalism should also have *legal ability*, i.e. to express concepts related to the legal world. We make the assumption that OWL has a high potential to be the language for such a formalism.

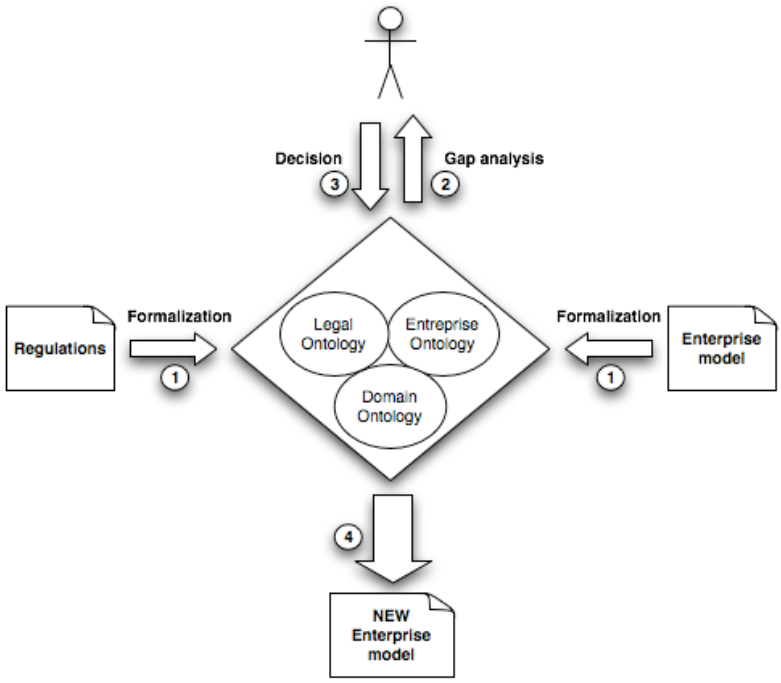

Fig 1. An ontology-based architecture for a DSS for requirements elicitations and enformcement.

For formalizing the Law, we plan to base our work on the legal ontologies efforts mentioned in our state of art review, specifically the LKIF since it's included in an ongoing and global European project(Estrella). A second ontology is needed to represent the enterprise model, i.e. the elements forming the business, application, information and technology levels of the enterprise. We are not aware of the existence of such an ontology, however inspiration could found be in some already known enterprise models frameworks like the TOGAF[20], Zachman framework[21], ARIS[22] or the SOA paradigm.

At last but not least, in order to express regulations and enterprise model about a given domain (banking, government institutions, insurance companies, etc…) a *Domain Ontology* is necessary to provide the concepts that are specific to the

concerned business area, i.e. for a bank it would be concepts like *client, trader, saving account, checking account, bill*, etc...

This high-level architecture is illustrated in the Fig.1. This decision-support system is based on the three ontologies already mentioned; it's the core that will provide the ability to compute the gap between two inputs: regulations and the enterprise architecture model. The system provides then a gap analysis (step 2), and the user - who would be the *accountable* person (IT compliance officer, requirements engineer, IT officer, etc…)- will decide on the change to do to the current enterprise architecture model (step 3). Finally the DSS provides as final output a new enterprise model that should be implemented (step4). This architecture should help compliance management in two aspects we mentioned above: the *traceability* since the gap is computed by formal logic, and *the holistic view* since our enterprise ontology would serve to represent the whole enterprise model, i.e. not only separate business processes.

Requirements enforcement

The second feature we want to address in our research question is the flexibility. We understand the flexibility of the IS as its ability to adapt to new requirements with minimum of time and cost, and above all in a way it stays integrated. Our hypothesis is that Model Driven Architecture[23] paradigm have a high potential to solve this problem. The solution is that the different ontologies used in the DSS (or at least the enterprise ontology) have to be compatible with the Meta-Object Facility (MOF) standard; a necessary condition for applying the MDA toolset. This track of research is currently investigated by the Object Management Group, and interesting work has already been done by [24] that translates for instance an ontology written in OWL to RDF language that would play the role of an export format to and from an MOF repository. This way, the system would generate from the *New enterprise model* in Fig.1 automatically a major part of the needed code. Traceability will here be extended to the IS components and would not be limited only to the enterprise model, since the code generation done formally.

2 Research Objectives

We divide our research in two folds:

a) **Requirements elicitations**: to develop an **ontology-based tool for gap analysis**. Here is the planned steps to build this tool:

- Design (or find) an **enterprise ontology** in OWL
- Extends the ontology LKIF with the enterprise ontology, so this entreprise ontology will have the legal dimension.
- Extends the enterprise ontology with an ontology for a given business domain, i.e. banking so we can reason about a given domain.
- To run a prototype: model some regulations concerning the banking domain (SOX) with the LKIF, inspired from the work done by the

Leibniz center [11](We might need to use in addition to the description logic in OWL a rule language).

The development will be divided in several iterations, at the end of every iteration an evaluation will update the tool requirements.

b) **Requirements enforcement**: extend the tool mentioned above with an MDA module.

- Investigate how the ontologies we have can be compatible with the MOF standard.
- Apply the MDA techniques to generate a Platform Specific Model (PSM).
- Evaluate the power of this approach, since we know that MDA doesn't generate 100% of the code (some parts have to be written manually).

4 Conclusion

In this proposal, we addressed the problem of desiging a traceable, formal, and holistic system for IS compliance management. Although several works addressed the two first features, we lack a system that provides a holistic approach, this is our motivation to propose the use of Enterprise models instead of processes models. In the other hand, though interesting formalisms were proposed to model regulations within some proposed prototypes, we believe that the use of the legal ontologies have a bigger potential since they were created specifically to address the problem of the law formalization and have chances to become electronic standards for law knowledge exchange. We already began to investigate the implementation of the first step of our architecture, and plan to validate it by with a real case with an partner in the industry.

References

1 Purdy, R. M. (2006) Compliance Initiatives Can Yield IT Opportunities. U.S. Banker. Retrieved from http://www.americanbanker.com/article.html?id=20060601WEM27QCJ&queryid=189565628&hitnum=1

2 IT Policy Compliance Group (2008) 2008 Annual Report: IT Governance, Risk and Compliance Improving Business Results and Mitigating Financial Risk. Retrieved May20, 2008 from http://www.itpolicycompliance.com/research_reports/it_governance/

3 Volonino, L., Gessner, G.H., Kermis, G.F. (2004) Holistic Compliance with Sarbanes-Oxley. Communications of the Association for Information Systems. 14(11): 219-233.

4 Hevner, A., March, S., Park J., Ram, S. (2004): "Design Science in Information Systems Research," MIS Quarterly, Vol. 28 No. 1, pp. 75-105.

5 Sheth, A. (2005). Enterprise Applications of Semantic Web: The Sweet Spot of Risk and Compliance. IFIP International Conference on Industrial Applications of Semantic Web (IASW2005), Jyvaskyla, Finland.

6 El Kharbili, M, Stein, S, Markovic, I, Pulvermueller, E. (2008). Towards a Framework for Semantic Business Process Compliance Management. GRCIS'08 Workshop at 20th International Conference, CAISE 2008, Montpellier, France.

7 Lau, G. T., Kerrigan, S. , Law, K. H. & Wiederhold, G. (2004). An E-Government Information Architecture for Regulation Analysis and Compliance Assistance. 6th International Conference on Electronic Commerce (ICEC), Delft, The Netherlands.

8 Giblin, C., Liu, A. Y , Müller, S. , Pfitzmann, B., & Zhou, X. (2005). Regulations Expressed As Logical Models (REALM). 18th Annual Conference on Legal Knowledge and Information Systems (JURIX 2005), IOS Press, Amsterdam.

9 Giblin, C.,Mueller, S. & Pfitzmann B. (2007). From Regulatory Policies to Event Monitoring Rules: Towards Model-Driven Compliance Automation. IBM Research Report, Zurich Research Laboratory

10 Gangemi, A., Prisco, A., Sagri, M.T., Steve, G., Tiscornia, D. (2003). Some ontological toolsto support legal regulatory compliance, with a case study. Workshop on Regulatory Ontologiesand the Modeling of Complaint Regulations (WORM CoRe 2003), Catania, Italy, Springer LNCS Catania.

11 Hoekstra, R., Breuker, J., Di Bello, M. & Boer, A. (2007). The LKIF Core ontology of basic legal concepts. Workshop on Legal Ontologies and Artificial Intelligence Techniques (LOAIT 2007).

12 Gangemi A. (2007). Design Patterns for Legal Ontology Construction. In P. Casanovas, P. Noriega, D. Bourcier, F. Galindo (Ed.), Trends in Legal Knowledge: The Semantic Web and the Regulation of Electronic Social Systems European Press Academic Publishing.

13 Rifaut, A. (2005). Goal-Driven Requirements Engineering for Supporting the ISO 15504 Assessment Process. Software Process Improvement, 12th European Conference, EuroSPI 2005, Budapest, Hungary, Springer.

14 Governatori, G., Milosevic, Z., Sadiq, S: (2006). Compliance Checking between Business Processes and Business Contracts. 10th IEEE Conference on Enterprise Distributed Object Computing.

15 Lezoche, M. (2008). Business Process Evolution: a Rule-based Approach. 20th International Conference, CAISE 2008, Montpellier, France.

16 Namiri, K., Stojanovic, N. (2007). A Semantic-based Approach for Compliance Management of Internal Controls in Business Processes. CAiSE Forum 2007.

17 Agrawal, R., Johnson, C., Kiernan, J., Leymann, F. (2006). Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. 22nd international Conference on Data Engineering., Washington, DC, USA, IEEE Computer Society.

18 Zur Muehlen, M., Rosemann, M. (2005). Integrating Risks in Business Process Models. Australasian Conference on Information Systems (ACIS 2005), Manly, Sydney, Australia.

19 Bonazzi R., Hussami L. & Pigneur Y. (2008) Compliance management is becoming a major issue in IS design. Italian chapter of the Association for Information Systems (ItAIS 2008). Paris, France.

20 The Open Group. The Open Group Architectural Framework (TOGAF), http://www.togaf.org/, http://www-128.ibm.com/developerworks/ibm/library/ar-togaf1

21 Zachman Framework, http://www.zifa.com/, http://www.zachmaninternational.com

22 Scheer, A.W.: ARIS - Business Process Frameworks. Springer, Berlin (1999)

23 The Object Management Group, http://www.omg.org/mda/

24 Carnefield S. & Pan J. (2007) Bridging the gap between the Model-Driven Architecture and ontology engineering. International Journal of Human-Computer Studies archive Volume 65 , Issue 7 (July 2007)