Compliance Management in Multi-actor Contexts

Riccardo Bonazzi[1], Yves Pigneur[1]

[1] HEC Lausanne, Institut de Systèmes d'Information, Internef
CH-1015 Lausanne - Switzerland
{riccardo.bonazzi, yves.pigneur}@unil.ch

Abstract. The main contribution of this paper lays in the idea of considering regulatory compliance management as a specific situation, where risks to mitigate are sometimes opportunities and where ambiguous and constantly changing requirements come from different stakeholders. We designed a solution and developed an artifact, which supports different users (namely business managers, compliance officers, and responsible of the Enterprise information system) achieving a shared agreement concerning the alignment between regulations and their information system. We will present how we are planning the test our solution in an enterprise by means of three scenarios.

Keywords: Governance, Risk, Compliance, Requirement Engineering.

1 Introduction

In this paper we intend compliance as "the act of adhering - and demonstrating adherence- to legal, regulatory and internal policies as well as of general market standards" (adapted from [1]). Should these policies and standards not be observed, "compliance risk" arises as, described by the main global regulator, the Basel Committee on Banking Supervision [2].

In recent years regulatory compliance has been seen worldwide by most enterprises as an increasing cost burden. The regulatory risk has even topped the list of business threats perceived by managers [3] although some studies (e.g. [4]) report an increase of performance for those who excel in compliance management.

The main challenge comes when an enterprise is subjected to multiple regulations, which have ambiguous, constantly evolving and sometime conflicting requirements. To give an example, one could mention the dilemma of a Swiss bank that has branches in United States. The Patriot Act is an American law that requires the Swiss bank to share data about its customers with American authorities to prevent terrorism; yet the Swiss bank has also to comply with the Swiss regulations concerning privacy. This re-regulation movement is expected to grow in amplitude in the following years, and compliance will increase its importance accordingly. In what concerns Enterprise Information Systems (EIS), there is a growing need for a solution that provides

automatic traceability for internal control, while assuring agility. To put in place a compliance information system is a fixed cost, while adapting it with the evolving regulations is a variable cost. Software is there to respond to different compliance needs [5] but it is up to the enterprise to clearly define its requirements, knowing that it does not exist yet a single Enterprise Governance, Risk and Compliance (GRC) solution.

In this study we take the point of view of the IT compliance officers of a financial institution. According to what we have been collected in our four-month internship, IT compliance officers have to take group decisions concerning the most profitable EIS under uncertainty in what concerns the evolution of regulations.

The current solutions to assure compliance against conflicting laws is to name compliance officers with expertise in international compared right and audit. Existing software helps IT compliance officers to monitor the processes of a company, yet it is up to each compliance officer to define the controls and the rules he requires. In doing so, the compliance officer is expected to have a clear understanding of law, business and Information Technology (IT) domains, in order to master a situation of negotiation between different stakeholders with different requirements. The expected solution should be economically sustainable, technologically feasible and legally compliant.

On top of that, a process analysis of the widely adopted quality-oriented approach shows that it mostly takes a reactive stance, which we believe does not help achieving efficiency and effectiveness. Indeed it requires too many controls and it acts only once the problem already exists, which does not assure it will be contained. Recent examples showed that society expects enterprise to adopt an ethical attitude, which does not limit itself on trying to control risky events, but that rather avoids taking risky paths.

We believe a quality management approach should be substituted by a risk management one. This way enterprise should seek for prevention, it should consider compliance as an issue while defining EIS requirements and it should collect opinions from experts in the three domains (law, IT, business) to obtain forecasts of the future.

In this sense systems to support group decisions have been proposed in the past years, yet they have missed integrating all the information coming from the EIS in one tool.

Moreover there has been a growing interest in defining which is the best type of relationship between regulator and the one who has to comply, the most recent analysis being McKinsey's Beardsley et al. [6]. Actor-Network theories (ANT) might help to understand how to satisfy different stakeholders' expectations, but we are not aware of any study in this sense being done in academic research on compliance management.

Concerning the requirement engineering side, the specificity of compliance management lays in the combination of ambiguous initial regulations, which have to be transformed into requirements by a group of stakeholders with different background and goals, in order to obtain a solution that assure efficiency and effectiveness, i.e. a reasonable trade-off between control and allowance of the business flow.

The main research question of this study is:

How to achieve IS compliance in a multi-actor context, such as EIS compliance to law in a financial institution?

That leads to the following sub-questions:

- What artifact would support the multi-actor and constantly evolving process of IS compliance management facing ambiguity, traceability and efficiency?
- How to best align regulations and IS to assure long term profitability?

The rest of the article will proceed as it follows. In section 2 we will illustrate the state of the art in compliance management support to identify which user's needs have not been fully addressed yet. This will allow us to introduce in section 3 our proposed artifact, which we have already developed. In section 4 we will propose three scenarios we intend to use to evaluate our artifact. Theoretical and practical contributions will be discussed in section 5, together with a presentation of our directions of investigation.

2 Background Literature in Compliance Management

In this section we present some of the previous works we referred to, while designing our artifact. We will start with the previous studies from literature and then we will give an overview of existing software one could implement. At the end of this section we will underline some holes in the existing research, which our solution is expected to adress.

To assess the existing literature we will use the framework proposed in Bonazzi et al. [7], which identifies the compliance function as composed of four steps: identification, assessment, enforcement and feedback. We prefer it against the GRC process proposed by Othersen et al. [8] as they refer to compliance only as a control function.

For what concerns compliance risk identification (step number 4 in figure 2.1) new ways to model regulations and retrieve them automatically have been proposed in the recent years. Legal ontologies would allow the users to gain from knowledge formalization and to allow access to multilingual and heterogeneous information sources, and some authors managed to harmonize requirements of different laws to assess the degree of compliance of a given situation. Yet there are methods that do not rely mainly on ontologies and do not consider inconsistencies as something to be avoided, like the Bagheri and Ghorbani's [9] viewpoints integration game, through which the inconsistencies of non-canonical requirement specifications are resolved.
The assessment step (step number 5 in figure 2.1) should follow the idea of holistic compliance proposed by Volonino [10]. Different users coming from the law, business and IT functions should gather and seek for a unique solution that satisfies all. One can mention recent works on Goal Oriented Requirement Engineering by means of i* based languages to express patterns to achieve compliance [11] and to

perform gap analysis between compliance needs and existing solution in place [12], the results of the gap analysis being the IS requirements. Otherwise the requirements could be expressed under shape of actions to be performed, as suggested by Breaux and Anton's [13] ontology-based extension of the Frame-Based Requirements Analysis Method. In this case Cheng et al [14] proposed a hierarchy between control activity objects.

On what concerns enforcement (step number 5 in figure 2.1) one could assume that the highest compliance risk is within the interaction between software applications, which could be seen as services. Hence compliance could then be enforced by means of Service Oriented Architecture (SOA). According to our understanding there are currently three major ways to ensure SOA policy management:

1. by means of business rules
2. by means of model driven methods
3. by formal methods like B-method or Alloy

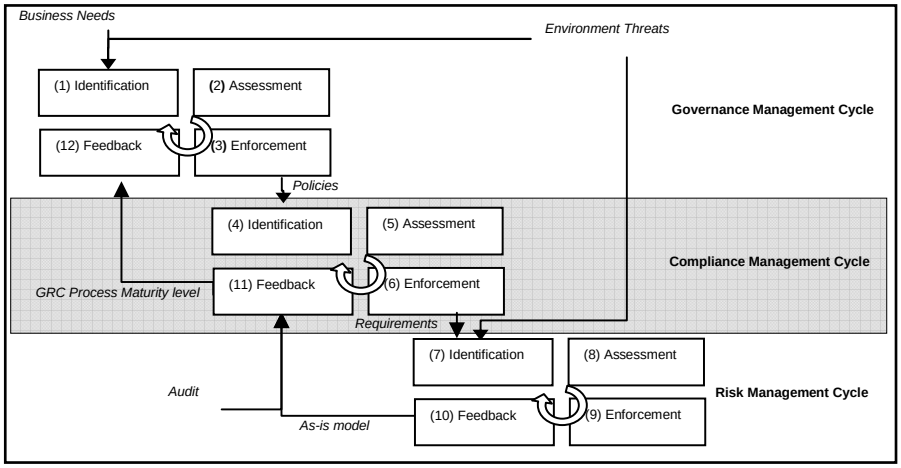

Figure 2.1: IT GRC process (source: [7]): the four-step compliance management cycle is in charge of aligning the Governance and the Risk Management cycles.

Finally the feedback step (step number 11 in figure 2.1) deals with visualization of the gap-analysis, and to do so one can follow the suggestions of Bellamy et al. [15].

Existing software that fully support the compliance management life cycle falls under two types:

Normative. GRC software, which seeks to enforce enterprise policies, that can be classed by means of four technology areas described by Rasmussen [16]: Enterprise Architecture, Enterprise Content Management, Business Intelligence and Business Process Modeling.

Heuristic. Those applications implementing supports the initial rule-driven approach by means of inference engines to allow adaptation to specific environments (e.g. the Autonomy's IDOL suite).

At the end we believe that the existing research has missed to spot three major issues, which we experienced during our internship:

The "risk" in business management is a requirement. There might be not such a thing as a "safe state" in an enterprise, as an enterprise that does not take risk might not get any profit. This is a difference stance compared to the spread opinion that to assure compliance we just need to add controls. The decision to comply with a regulation should be rather seen as an option, which has a cost and that shall lead to future profits.

Accountability is shared in a large enterprise, hence compliance should be considered as a shared requirement. We do not share the idea of seeing the compliance requirements engineering as a waterfall process, which starts with a law expert and ends with the IT platform responsible. We believe that the alignment between Law and IT should be done in a way that merges the viewpoints of business managers, compliance officers and IT risk managers. Referring to Van de Ven and Poole[17] we wish to extend the focus of GRC theories beyond the single entity (i.e. one actor) towards the multiple entities (a business manager, a compliance officer, and responsible of the Enterprise information system). This appears to us as a situation where all actors gain by cooperating, even if they have different goals, as the one described by Nalebuff and Branderburger [18].

Compliance should be rather seen as a question of alignment rather than a simple matter of control. Many experts agree that a set of compliant processes does not assure that the way business is conceived will be compliant. As previously mentioned compliance is perceived by many enterprises as a strategic threat, hence the alignment between law and IT should include the enterprise business model. We also believe that a business model that complies with regulations should require fewer controls at the process level, since most compliance risks are prevented by avoidance while designing the processes themselves.

To address such issues one could deploy a system to support and trace shared decisions between stakeholders, seeking a good balance between risk mitigation and profitability, and representing it at the business model level.

3 Designing a Compliance Support System

In this section we will describe our designing goals and the analysis we performed before creating the artifact.

3.1 Problem Analysis and Our Goals

Figure 3.1 illustrates the main concepts of the compliance problem and their influences on each others. A plus on an arrow underlines a proportional relationship between two concepts (if A increase, then B increases), while a minus implies an

inverse relationship (when A increases, B decreases). Hence one can notice that "regulations" like SOX are the consequences of "incidents", e.g. the Enron scandal. To increase "controls number" is the current solution to achieve a high "compliance degree", as it reduces the "risk" of incident while it increases the cost for the enterprise. Too many regulations might increase "disagreements between stakeholders" (e.g. how to put in place a sustainable solution to with SOX) which increases the risk of a new accident, e.g. if they disagree and start each stakeholder adopts ad-hoc solutions.

In designing our artifact we aim at obtaining an Integrated Decision Support System for a set of coopetitve users. In its final stage it shall adopt semantic technologies to assist compliance risk management, to automatically assess the compliance degree of an Enterprise Information System (EIS) and to help enforcing the required actions. Our artifact should diminish "disagreements between stakeholders". The results would be a proactive approach aiming at reducing "risk" with a lower number of controls, which leads to a lower "cost" for the same compliance degree. In the next section we will describe how we plan to evaluate these achievements.

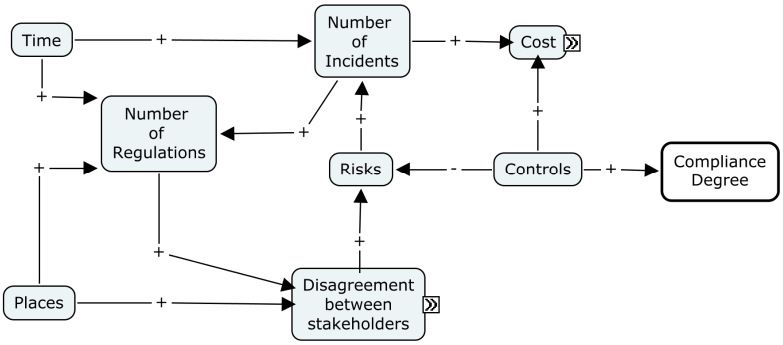

Figure 3.1: Problem analysis

3.2 The General Design of the Artifact

The figure in appendix represents the result of our time spent with the IT compliance officer of the financial institution, whose data have been moved from the image to respect confidentiality.

One can identify a list of boxes of different sizes. The big boxes are a sort of "libraries", i.e. a list of objects available. The user can draw the link between components of different libraries (e.g. a regulation like SOX and the Business unit USA) by adding a small box within a big one (e.g. by adding a small box called SOX within the business unit USA's box). This way the traceability is assured while IT issues are hidden to the most users, who can discuss mainly about the way to align IT services and law/business requirements.

The Top Part of the Figure. The business level of the company is represented, with the collection of business entities, which are composed of business units. The small squares refer to the regulations, which each business line and entity is submitted to. If a business entity is submitted to a regulation, all its business units inherit the compliance need. In the original design different colors of the square boxes represent the level of compliance risk exposure after the gap analysis has been performed. Hence a business unit in Japan might be submitted to J-SOX, the Japanese version of SOX, and it might get a red box if it does not comply yet, while the business unit in USA gets an orange box about SOX if a started project to comply with the law has not finished yet.

The Middle Part of the Figure. A collection of regulations is presented. Each regulation box shows an ID, the name of the regulation and the control activities required.

The control activities have their own ID expressed in a circle. The color of the circle tells if the control activity is conceived to reduce the risk by requiring a preventing, proactive or reactive stance. This way Sarbanes-Oxley might have "SOX" as ID, and it might require "assure internal control" as control activity, which is a preventing/proactive activity. To define the control activities we referred to COSO and CobiT.

The Bottom Part of the Figure. The IT solutions currently owned by the enterprise find place. Each IT solution is conceived to support at least one control activity. Thus Enterprise GRC software, like BWise, might support the activity "assure internal control".

3.3 The Data Objects

As previously mentioned, for the compliance risk identification we followed the idea of compliance management as an alignment function between four domains, which we represented as four different data sources. That led us to design a distributed application, which allow different user to perform different kinds of actions while sharing knowledge during the compliance management life cycle.

In our current stage of development, we have been focusing on the server side, which will be described, hereby more in details. Each data type is associated with a different data object. We refer to the problem analysis shown in figure 3.2 to illustrate the data objects we used for the prototype. For simplicity we have been using so far data coming from static text files, but we will switch now to data coming from data streams. We assumed that data are coming from reliable sources, while the links between data objects are subject of disagreement between stakeholders.

For the "Business unit" object, we considered as source the output delivered by the business model computer aided design tool proposed by Fritscher [19].

For the "Regulation" object, we supposed to receive a source within the existing regulatory and risk content feeds such as Complinet, Economist Intelligence Unit, LexisNexis, and Thomson Reuters. Each regulation object refers to a written

document, which is described by means of its name, the location where it is applied, the enforcement date, and the cost of non-compliance.

For the "IT Solution" object, we supposed to receive one of the existing solutions benchmarks ("Hype-cycle" or "Wave") done by Gartner, Inc. and Forrester Research, Inc. Each IT solution is associated with a cost object, which is the sum of fixed and variable cost.

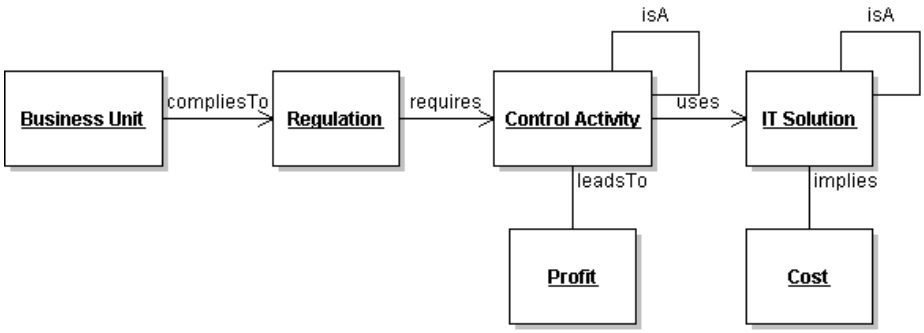

Figure 3.2: Data Objects

We have also defined another object, called "Control Activity", which recalls the idea of "patterns" of Compagna et al. [11], as well as the "legal annotation" of Breux and Anton [13]. Control activities are rules, which we suppose will be given to another system to perform inferences. An action is composed of a verb and an object, which refers to an informal ontology that we have developed referring to COSO Enterprise Risk Management framework and CobiT. Hence "store communication data" is an action. Actions have parameters to express modes and time. This way "store [WORM] (5 years) communication data" would require a Write-once Read-many storage to retain for five years communication data. The novelty of our approach concerning the actions extends the idea of hierarchy mentioned by Cheng et al [14]. This way "store mail" is a subset of "store communication data". Control activities might lead to economic returns as a consequence of increased operational quality, as suggested by [4].

The associations between data objects follow the viewpoints of the stakeholders. Referring to Bagheri and Ghorbani's [9] we expressed the subjective opinions of stakeholders by three parameters (belief, disbelief and uncertainty), i.e. how much they are sure the statement is correct, how much they are sure it is not correct and how much they wonder whether the statement is correct of incorrect.

3.4 Functions of the System

The artifact has three main functions: it retrieves information from the four sources; it presents it to the user; it collects new data from the users and updates the four sources accordingly.

The Data Retrieval. This is done periodically on the server side. Each data source is composed of a body containing the data objects and a header with a summary of the data objects contained. Thus in a regulation source containing information about Sarbanes-Oxley, Patriot Act and Basel II in its body part, one shall retrieve from its header a string "SOX-PA-Basel II".

The Data Presentation. This is done on the client side. It starts when the client, who has received the four headers, requests more information about a specific data object (e.g. the business unit in USA). The client receives from the server the information about the business unit, the regulations it has to comply with, the actions required by the regulations and the IT solutions to enforce the actions. Data analyses (for example those concerning the degree of compliance of the business unit) are then done on the client side.

The Update Function. It starts when the user adds a link between two data objects (e.g. Business Unit of USA with Basel II regulation). The user is asked to determine his degree of certitude (sure, almost sure, what-if analysis) associated to the link he added. The request to update is sent to server, which stores it in a log with the entire requests for the same link. The degree of agreement between different positions is then examined: if all position agrees on the existence of the link, the update is made effective and all users are notified. If there no agreement between stakeholders an issue is raised to the attention of the stakeholders involved and a possible solution is proposed.

4 Evaluation with Case Studies

In this section we will present how we intend to perform the validation of our artifact. We will present a set of evaluation criteria and few scenarios, which we believe a compliance management support system should be able to address.

4.1 Our Evaluation Criteria

According to our research question, we defined the following set of evaluating criteria, which we wanted to satisfy.

*Agility***.** Regulations require a flexible approach to deal with their constant evolution. Hence how does the artifact react when requirements change over time? (We will measure it in terms of actions required for the user).

*Conflicts resolution***.** Due to the ambiguity of regulation, different points of view of users involved have to be harmonized. In addition to that, different laws might apply to the same enterprise, which has to harmonize their requirements. How does the artifact resolve such conflicts? (We will measure it in terms of conflicts resolved against the overall viewpoints)

*A standard language***.** A common ground is required to assure common understanding of all users involved. Which degree of standardization the artifact adopts? (We will ask the users to define if they felt constrained by the terms used).

Automation. While seeking to increase cost efficiency a greater degree of control automation reduces the risks linked to internal employees. Which degree of automatic tasks is executed in the overall workflow? (We will measure it in terms of automatic tasks executed against the overall number of task, together with the time required to execute our process against the traditional way).

Accountability. A certain amount of decisions will have to be taken by users and not by the artifact, to assure accountability in case of accident. How does the artifact support such decisions and how does it assure accountability? (We will measure it in terms of decisions, which we can assign to a specific user being accountable, against the overall amount of decisions).

4.2 Scenario 1: Performing a Gap Analysis

A compliance officer usually needs to have a quick overview of the existing situation concerning compliance in a determined business unit. Once the system has been started, the compliance officer can select a business unit from the menu to have the list of required IT solutions that are yet to be implemented, together with the expected cost the enterprise will have to face. Table 4.1 illustrates how we expect the artifact to react in this scenario.

Table 4.1: Performing a gap analysis

Goal	To perform Gap Analysis	
Preconditions	Indexes already retrieved	
Success End Condition	The user obtains the list of IT solutions required to comply with the existing regulations, which the business unit is submitted to	
Failed End Condition	The user does not receive the list of IT solutions The list is not correct	
Primary Actor	User (Business manager; compliance officer; IT employee)	
Trigger	The user starts the Compliance Support System	
DESCRIPTION	1	Server collects the headers from the data sources
	2	Serve sends the header to the client
	3	Client selects the business unit USA (BU1) from the business units list
	4	Client Request data objects for (BU1)
	5	Server sends data objects (Business Unit, Regulations, Actions, IT solutions)
	6	Client performs gap analysis
	7	Client resents results (Cost)

4.3 Scenario 2: Adapting Different Viewpoints of a Regulation Requirements Once a New Interpretation of the Law Comes In

The user can affect a new regulation towards the business units, which he beliefs will be concerned by the new law. An estimation of his degree of is required to help harmonizing his assessment with the ones of the other users. The belief of the user is stored in a log file and merged with belief of other users on the same matter. If the sum of belief involves a compliance risk that is greater than the risk appetite of the company, the regulation is added to the business unit, and a new gap analysis is performed. The viewpoints inconsistent between users will be highlighted in the dashboard of the interested users. Once the requirements are harmonized the set of required tools that minimizes the cost will be proposed, together with the list of expected profits coming from the introduction of new control actions. Table 4.2 illustrates how we expect the artifact to react in this scenario.

Table 4.2: Adapting regulations requirements

Goal	To adapt requirements of a regulation	
Preconditions	Company risk appetite already defined. Compliance officer has been informed of a new interpretation of SOX.	
Success End Condition	The user updates the regulation requirements and the business units are automatically affected	
Failed End Condition	The user cannot update the regulation requirements The business units are not automatically affected	
Primary Actor	Compliance officer	
Trigger	The user selects the business units USA and the regulation SOX	
DESCRIPTION	1	Client defines his degree of certitude (Almost sure) for the link business units USA - SOX
	2	Server stores the information in a log
	3	Server merges all the beliefs regarding the association business unit USA with the regulation SOX
	4	Server compares the overall belief (90% that the USA business line has to comply with SOX) with the risk appetite of the company (1%)
	5	Since 90%>1% server updates the information in the file of Business Unit USA
	6	Server sends updated data objects (Business Unit, Regulations, Actions, IT solutions)
	7	Client performs gap analysis
	8	Client presents results (Cost, profit)

4.4 Scenario 3: Dealing with Future Regulation Requirements

Most strategic decision are done concerning the future, hence the users can add links, which are yet to come. In this case their degree of certitude will be lower.
Thanks to the temporal dimension linked to the regulations, the system automatically splits them into “existing” and “to come”. This way a compliance officer might add today to the business unit USA a regulation that will apply in 2010. This way the IT employee will have time to adapt the IS infrastructure, which has an impact on the

installation cost, since it is not done under emergency. This type of forecast allows what-if analysis, whose links are stored in the log with a low degree of certitude. Table 4.3 illustrates how we expect the artifact to react in this scenario.

Table 4.3 Dealing with future regulations requirements

Goal	To perform what-if analysis	
Preconditions	Compliance officer has intended a rumor of a new regulation for the USA.	
Success End Condition	The user updates the regulation requirements adding a future date and the others users gets notified.	
Failed End Condition	The user cannot update the regulation requirements by means of a future date The others users do not get notified	
Primary	Compliance officer	
Trigger	The user adds a new law called X and sets the due time as "2010"	
DESCRIPTION	1	Client defines his degree of certitude (Almost sure) for the link between business units USA and regulation SOX
	2	Server recognizes that it is in the future
	3	Server updates log, merge beliefs and send updated data
	4	Client recognizes that it is in the future
	5	Client performs gap analysis (current)
	6	Client performs gap analysis ("to come")
	7	Client presents results (Cost, profit)

5 Conclusions

We conclude this article with the discussion of findings and contributions before moving towards limitations of the study together with hints for future works.

5.1 Discussion of Findings and Contributions

In this study we wanted to design a solution to support the multi-actor and constantly evolving process of IS compliance management face ambiguity, traceability and efficiency. The way we developed our artifact presented a new approach towards compliance, which seeks at facilitating a proactive stance by introducing the temporal dimension together with the uncertainties of multiple stakeholders.
Referring to [17] our theoretical contribution takes into consideration both the "prescribed" and the "constructive" mode of change at the single entity level, i.e. the life-cycle and the goal oriented approached, and extends towards the multiple entities level by adding the "dialectic" mode of change, i.e. the negotiation between stakeholders, which we believe should be considered as a strategic task. To make our design falsifiable we develop a prototype and outlined how we are planning to evaluate it by means of scenarios.

The propositions we aim at verifying with the validation are the following:

Agility. A change in the environment automatically triggers a new analysis of the overall information system architecture and delivers a new set of requirements which maximizes the utility function (in our case the required expenses).

Conflicts resolution. Viewpoints allow merging the requirements of all stakeholders. Conflicting regulations are analyzed on the base of the IT tools they required, which allow us to do quantitative comparison (e.g. the overall cost of the IT tools to buy, in each option).

A standard language. The use of viewpoints limits the needs of an ontology and allows user to express their beliefs in the first stage. Users can add new objects, which shall be used by all stakeholders. After each rounds of the merging game a common language emerge between the users. This way only those new objects, which are effectively used, will be kept in the server.

Automation. Referring to figure 2.1 our artifact supports the Identification, Enforcement and Feedback steps. The Assessment part is left to be performed by the user, since it requires decisions, while the system simply records the choices to assure accountability.

Accountability. The viewpoints method allows us to obtain the solution, which will reduce the risk of conflicting goals between stakeholders. Each viewpoint is recorded, hence it is possible to define how decided what.

5.2 Limitations and Further Works

As previously mentioned in the current stage of software development our assumptions are based on the data we collected during our internship. This is why we have planned to test the artifact in the following months. Also, in this phase of software development we focused on the best way to support and trace decisions in a multi-actors context. In the following phases we plan to extend the functionalities of the artifact in the following domains:

Distributed architecture. We plan to improve the way concurrent tasks are handled, and how the server and the clients exchange data.

Data collection from real sources. Real data stream will be merged together

Use of semantic technologies. A meta-level will be needed to merge different data stream, and we believe we could use the result of this operation to use a reasoner.

Decision support. The final artifact shall be able to optimize the utility function, as presented by Muller and Supatgiat [20].

Automatic enforcement. A parallel study in our institute [21] is in charge of developing the extension of our prototype towards an automated, predictive run-time monitoring system that tells what is expected of an institution, given the regulations and the current situation.

Improved usability. This will mainly regard the client side, but we expect it to have consequences on the server side as well.

References

1. McClean, C., Rasmussen, M.: Topic Overview: Governance, Risk And Compliance. (2007). Available at http://www.forrester.com
2. Basel Committee on Banking Supervision: Compliance and the compliance function in banks (2005), http://www.bis.org/publ/bcbs113.pdf
3. Economist Intelligence Unit: Regulatory Risk: Trends and Strategies for the CRO (2005).
4. IT Policy Compliance Group: Annual Report: IT Governance, Risk and Compliance – Improving Business Results and Mitigating Financial Risk (IT Policy Compliance Group, 2008). Available at http://www.itpolicycompliance.com/research_reports/it_governance/.
5. McClean, C.: The GRC Technology Puzzle: Getting All The Pieces To Fit (2009). Available at http://www.forrester.com
6. Beardsley, S., Enriquez, L., Nuttall, R.: Managing regulation in a new era. The McKinsey Quarterly, 90--97 (2009).
7. Bonazzi, R., Hussami, L., Pigneur, Y.: Compliance management is becoming a major issue in IS design. In: D'Atri, A., Saccà, D (eds.) Information Systems: People, Organizations, Institutions, and Technologies, In press. Springer (2008). Available at: http://tinyurl.com/grc-dss
8. Othersen, M.: Cutting Through The IT GRC Hype (2008). Available at http://www.forrester.com
9. Bagheri, E. & Ghorbani, A.A.: The Analysis and Management of Non-Canonical Requirement Specifications through a Belief Integration Game. Accepted Knowledge and Information Systems: An International Journal (2009). Available at: http://glass.cs.unb.ca/~ebrahim/papers/kais.pdf.
10. Volonino, L., Gessner, G.H. & Kermis, G.F.: Holistic Compliance with Sarbanes-Oxley. The Communications of the Association for Information Systems, 12, 457--468 (2003).
11. Compagna, L., El Khoury, P., Krausová, A., Massacci, F., Zannone, N.: How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. Artificial Intelligence and Law, 17, 1--30 (2009).
12. Rifaut, A. & Faltus, C. Improving Operational Risk Management System by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach (2006).
13. Breaux, T.D. & Antón, A.I.: Managing Ambiguity and Traceability in Regulatory Requirements: A Tool-supported Frame-based Approach, (2007). Available at ftp://ftp.ncsu.edu/pub/unity/lockers/ftp/csc_anon/tech/2007/TR-2007-26.pdf
14. Cheng, C.P., Lau, G.T., Law, K.H., Pan, J., Jones, A.: Regulation Retrieval Using Industry Specific Taxonomies, Artificial Intelligence and Law, 16, 277--303 (2008).
15. Bellamy, R.K.E. et al.: Seeing is believing: Designing visualizations for managing risk and compliance. IBM Systems Journal, 46(2), 205--218 (2007).
16. Rasmussen, M.: Overcoming Risk And Compliance Myopia, (2006). Available at http://www.forrester.com
17. Van de Ven, A.H. & Poole, M.S.: Explaining development and change in organizations. Academy of management review, 520 (1995).
18. Nalebuff, B. & Brandenburger, A.: Co-opetition: Competitive and cooperative business strategies for the digital economy. Strategy & Leadership, 25(6), 28--35 (1997).
19. Fritscher, B.: Business Model Designer From Sticky Note To Screen Interaction. (2008). Available at: http://www.fritscher.ch/hec/projets
20. Muller, S. & Supatgiat, C.: A quantitative optimization model for dynamic risk-based compliance management. IBM Journal of Research and Development, 51(3), 295--308 (2007).
21. Hussami, L: A decision-support system for IS compliance management (2009). Available at: http://tinyurl.com/grc-dss1

Appendix: The design of the artifact's interface