Compliance management is becoming a major issue in IS design

R. Bonazzi, L. Hussami, Y. Pigneur[1]

Abstract This article aims at improving the information systems management support to Risk and Compliance Management process, i.e. the management of all compliance imperatives that impact an organization, including both legal and strategically self-imposed imperatives. We propose a process to achieve such regulatory compliance by aligning the Governance activities with the Risk Management ones, and we suggest Compliance should be considered as a requirement for the Risk Management platform. We will propose a framework to align law and IT compliance requirements and we will use it to underline possible directions of investigation resumed in our discussion section. This work is based on an extensive review of the existing literature and on the results of a four-month internship done within the IT compliance team of a major financial institution in Switzerland, which has legal entities situated in different countries.

1 Introduction

In this article we suggest that compliance requires a multifaceted alignment, which should be treated in the early steps of Information Systems (IS) engineering at a higher level than the applicative one, to assure the flexibility required to deal with the evolution of laws.

Addressing risk and compliance management means acknowledging the larger re-regulation movement, started in the 1990s. Observing this evolution with concern, several industry experts warn about the negative consequences of the "regulatory overload" or "regulatory burden". One of the main reasons compliance with regulation is considered as being a burden is its cost (e.g. [1] shows how compliance performances affect enterprise costs). Top cost drivers in the area of risk and compliance management are IT systems, i.e. data processing and corresponding software.

1 HEC Lausanne, Institut de Systèmes d'Information (ISI), Lausanne, Switzerland, riccardo.bonazzi@unil.ch, lotfi.hussami@unil.ch, yves.pigneur@unil.ch

The trouble comes from the implementation approaches selected by most of the companies, which continue to meet compliance requirements “with one-off, best-of-breed solutions that address today's immediate need” [2], without an integrative architectural approach. All experts observe that an integrated compliance management approach is required for complying with multi-source, evolving and complex regulations (e.g. [3][4][5]). A global or holistic compliance requires a “Governance, Risk and Compliance” approach, which we applied in proposing a so called “IT GRC process” illustrated in figure 1.1 and composed of steps in three loops, which turns at different speed and that we associate at two watches (Governance and risk management loop) and one coordination system (Compliance management loop). The time of the watches is the IT GRC proces maturity level required.

Each loop has four steps: the first one identifies the threats, the second one assesses them and decides which ones to address. The third one puts into place artifacts to enforce the decisions taken in the previous steps. The fourth step gives feedback to the identification step.

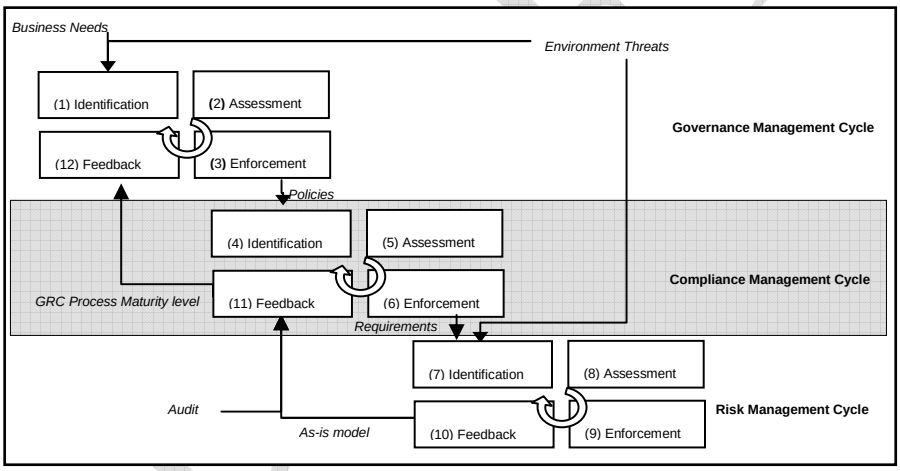

Fig. 1.1 IT GRC process

More in details, the first three steps shown in figure 1.1 belong to the Governance loop, i.e. “the act of establishing IT decision structures, processes, and communication mechanisms in support of the business objectives and tracking progress against fulfilling business obligations efficiently and consistently”, according to [6]. Steps 4, 5 and 6 belong to a coordination loop and deal with compliance, “the act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies and procedures”, according to [7]. Steps 7, 8, and 9 belong to the risk management loop, “a coordinated set of activities to not only manage the adverse impacts of IT on business operations but

to also realize the opportunities that IT brings to increase business value", according to [6]. Steps 10, 11 and 12 are the feedback steps of each loop.

The article proceeds in the following way. Section 2 presents a framework to perform the alignments required by compliance. Section 3 describes in details each alignment by citing existing example in the IS literature and underlining zones that are not fully covered yet. Section 4 concludes with discussion and further works.

2 IT Compliance framework

For our IT GRC process model we combined the concept of a risk management cycle [8] and the ones of quality management [1] together with the previous works of Giblin et al. [9] of IBM, Sheth [10] from Semagix and El Kharbili et al. [11], who proposed a compliance process life-cycle and described the process steps. Giblin [11] described a possible holistic solution, yet it seems that the compliance problem has two dimensions – *Legal Dimension* and *IT Dimension*-, while there are two kinds of sources of regulations to comply with: *External* and *Internal*.

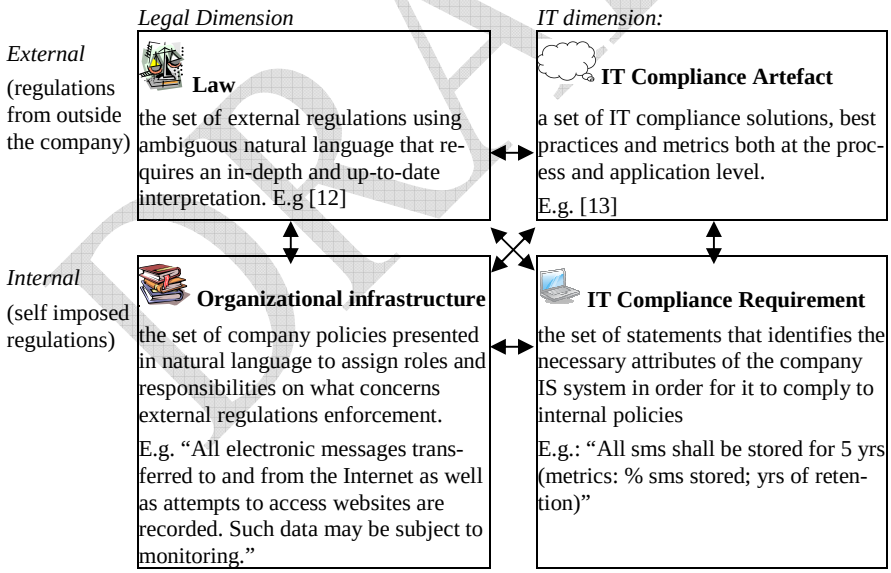

Fig. 2.1 Regulation / IT alignment

We propose the regulation/IT alignment framework illustrated in Figure 2.1. This is aimed to recall the strategic alignment model of Henderson & Venkatraman [14] and it has four domains, as the product between dimensions and sources of regulations. For the sake of clarity, figure 2.1 presents a real example taken

from practice, concerning requirement engineering for document retention compliance with SEC 17a-4. Comparing figure 2.1 with figure 1.1, one can notice that the Governance steps of the IT GRC process generate the policies in the Organizational Infrstructure, while the Compliance steps deliver the IT Compliance Risk Management infrastructure.

3 Different alignments between domains

This section describes the different alignments in the framework presented in figure 2.1, under the assumption that an arrow in the picture corresponds to two alignments in opposite directions. Each alignment refers to a brief review of articles both from the academic journals and from research groups like Forrester Research, Inc. and Gartner, Inc.

The alignments between the Law domain and the Organizational Infrastructure domain. We named the effort aimed at aligning the Organizational Infrastructure with the Law as **contextualization**. It concerns the first three steps of the IT GRC process and it is the subject of frameworks like COSO [15] for what concerns enforcement strategies. A support tool for the identification and assessment parts is proposed by Lau et al. [16], i.e. a hierarchical taxonomy of regulations using a XML structure, coupled with a reasoner as a compliance checking assistant that asks to the user a set of questions in order to define whether he is compliant with the law.

On the other direction of the arrow we named the effort aimed at aligning the Law with the Organizational Infrastructure as **Contracting**, which concerns steps 12 of the IT GRC process and is mostly the subject of journals for compliance officers (e.g. [17]). For this activity we did not find any IT support artifact.

The alignments between the Organizational Infrastructure domain and IT Compliance requirement domain. We named the act of defining the IT compliance requirements starting from the company policies as **To-be analysis**, since it involves the design of the new IS. This can be treated in different ways, depending if one sees it as a set of controls to put into place (e.g. CobiT [18]) or as a number of IT risks to adress (e.g. ISO 17799). We defined three kinds of design solutions:

Ex-post solutions to design an artifact to assess the level of compliance. Rifaut [19] proposed a Goal-Oriented Requirement Engineering (GORE) framework based on the ISO 15504 standard for process assessment to ease the checking task and define the maturity level of a process. Governatori et al. [20] 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. Lezoche et al. [21] studied 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; thus one could also see it as an ex-ante solution.

On going solutions to design an artifact that could assure a real time internal control. Namiri & Stojanovic [22] from SAP proposed the implementation of the Internal Control process as semantic layer above business processes, called Semantic mirror, which contains the rules under which the business process can be executed, and are derived from the risk assessment of the business process. A related work is Agrawal et al. [23] from IBM, who proposed to see 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.

Ex-ante solutions to design an artifact aimed at avoiding actions that are not compliant. Zur Muehlen & Rosemann [24] proposed an approach to design and model business processes by considering the risks they are exposed too. The result is a business process model that encompasses the risks, by means of three elements: a risk taxonomy, a taxonomy of the business process elements exposed to risk and a set of risk handling strategies.

On the other direction of the arrow, in order to align the Organizational infrastructure with the IT compliance requirements one could find inspiration from the authors grouped in the “ex-post solutions” (i.e. [19], [20], [21], [22], [23]) to perform an as-is analysis of the existing IT capacities before listing the actions required. This is why we decided to name this alignment as **As-is analysis**.

The alignments between the IT artifacts domain and IT Compliance requirement domain. The act of defining the IT compliance requirements starting from the existing IT artifacts is here named as **Artifact Choice**. The support artifact could be under the shape of studies from Universities or of vendors/products comparisons offered by research centres, as well as strategic advices coming from an external consultant. On the application level the new compliance demand yields the thinking and the design of different types of applications to support compliance and risk management (Heiser et al. [25] offered a list of the most important in 2008). Assuming that information is the cornerstone of any effective risk & compliance process, Sheth [10] argued that semantic technologies are a good support for compliance applications.

On the other direction of the arrow the effort aimed at aligning IT artifact with the IT Compliance requirements of companies could be named as **Trends Analysis** and it might lead either to a case study (e.g. [4]), to a set of best practices (e.g. [6]) or to a new version of an IT application.

The alignments between the Law domain and the IT artifact domain. The act of aligning IT artifact with the Law could be called Artifact **Creation**. Most of this effort is still under the shape of tacit knowledge and we could only find effort aimed at formalizing the law, which is the first step in order to develop an artifact according to [9], [10] and [11]. Gangemi et al. [26] built a Core Legal Ontology

(CLO) above an extension of their previous work DOLCE. Another considerable effort has been made by Hoekstra et al. [27] of the Leibniz center for Law who built the LKIF ontology for describing legal concepts over 3 layers (abstract, basic and legal).

In the other direction we found only few authors who treated the alignment between Law and the existing IT artifacts (e.g. Gasser's analysis of *dynamization of the law* [5] or Skinner's idea of *forensically evolving regulations* [28]). We decided to call this alignment **Awareness**.

The diagonal alignments. Even if many authors (i.e. [1], [3], [6], [9], [10], [11]) have already envisaged an alignment of IT requirements with the Law yet these applications are to come. On the opposite direction of the arrow, nothing has been found on the alignment of law with the solutions implemented in companies.

We did not find much concerning the IT artifact/Organizational Infrastructure alignment, even if one could suppose to use the framework from Hevner et al. [29] to obtain rigor (Support choice alignment) and Relevance (Assessment). On the other direction of the alignment (Organizational Infrastructure/ IT artifact) one could suppose an artifact that would allow a company to define the policies by being aware of the existing IT artifacts.

4 Discussions and further works

Based on an analysis of the state of art, we can notice that several alignments efforts have been done separately without a holistic view ([3], [4]); we propose these research axes:

1) A holistic system: as we mentioned, one could think about bringing all the isolated efforts together. Considerable work was achieved for legal ontologies (CLO, LKIF); we can go further by putting them in the context of a compliance management system. The efforts by [22], [23] and [24] at the business process level form a package and need to be integrated together. A coupling with a risk assessment tool [22] is needed for a GRC process, and then the whole should be linked with a legal assistance tool. In a first moment a common formalism that aligns the legal, business and IT concepts should be elaborated. This will give the compliance dimension for an organization business model where we would see the impact trace of a regulation on the business, process and application levels. This model would be of high usefulness to support decision making and auditing. Finally the system should achieve a high flexibility to assure constant evolution. Different layers of abstractions are then needed and we suggest an investigation on the combination of ontologies and the Model-Driven Architecture paradigm.

2) Support to alignment decisions: the different alignments required by compliance need an approach that goes beyond solving classical ambiguity or contradictions handling between actors involved. The specificity of the legal context in-

volves more or less voluntary asymmetry of information between parties interested. Starting from the idea of an artifacts aimed at solving classical ambiguity or contradictions handling (e.g. the legal use cases proposed by Gangemi [30]) one could study different cases of "coopetition", in which actors have interest of cooperate and compete at the same time, to determine the effect asymmetry of information on the perception of risk and the amount of wrong estimations done. Then, assuming that a common language for alignment is available, it would be interesting to see the different usages of such language that each actor does, according to his specific goals. This would help designing a support system for group decisions, which would implement the holistic system features described in the previous point.

References

1. 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/
2. 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
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. Rasmussen, M. (2005). Seven habit of highly effective compliance programs. Retrieved from http://www.forrester.com/Research/PDF/0,5110,37240,00.pdf.
5. Gasser, U., Hausermann, D. M (2007). E-compliance: Towards A Roadmap For Effective Risk Management. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=971848.
6. Kark, K., Othersen, M. & McClean, C. (2007). Defining IT GRC. Retrieved from http://www.forrester.com/Research/PDF/0,5110,43341,00.pdf.
7. McClean, C., Rasmussen, M. (2007). Topic Overview: Governance, Risk, And Compliance. Retrieved from http://www.forrester.com/Research/PDF/0,5110,39611,00.pdf
8. Her Majesty Treasury (2004). The Orange Book. Management of Risk - Principles and Concepts. Retrieved from http://www.hm-treasury.gov.uk/media/3/5/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf
9. 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.
10. 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.
11. 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.
12. Security And Exchange Commission (1993) Reporting Requirements for Brokers or Dealers under the Security Exchange Act of 1934. Retrieved from http://www.sec.gov/rules/final/34-38245.txt

13. Federal Rules of Civil Procedure (2007). Rule 34 (a). Retrieved from http://www.law.cornell.edu/rules/frcp/Rule34.htm
14. Henderson, J. C., Venkatraman, H. (1993). "Strategic alignment: Leveraging information technology for transforming organizations." IBM Systems Journal 32(1): 472-484.
15. COSO (2004) Enterprise Risk Management Integrated Framework- Executive Summary.. Retrieved from www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf
16. 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.
17. Maher, M. M. (2005). "Tips for Managing Relationship with Regulators." ABA Bank Compliance 26(3): 24-28.
18. ISACA (2007) Control Objectives for Information and related Technology (COBIT) 4.1. Retrieved from http://www.isaca.org
19. 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.
20. Governatori, G., Milosevic, Z., Sadiq, S: (2006). Compliance Checking between Business Processes and Business Contracts. 10th IEEE Conference on Enterprise Distributed Object Computing.
21. Lezoche, M., Missikoff, M., Tininini, L. (2008). Business Process Evolution: a Rule-based Approach. 20th International Conference, CAISE 2008, Montpellier, France.
22. Namiri, K., Stojanovic, N. (2007). A Semantic-based Approach for Compliance Management of Internal Controls in Business Processes. CAiSE Forum 2007.
23. 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.
24. Zur Muehlen, M., Rosemann, M. (2005). Integrating Risks in Business Process Models. Australasian Conference on Information Systems (ACIS 2005), Manly, Sydney, Australia.
25. Heiser, J., Perkins, E., Witty, R.J., Williams, B., Miklovic, D., De Lotto, R.J., Vining, J., Van Decker, J.E., Colville, R.J., Nicolett, M., Stevens, L., McKibben, D., Furlonger, D., Caldwell, F., Proctor, P.E., Chin, K., Logan, D., Ouellet, E., Wheatman, J., DiCenzo, C., McDonald, N., Bace, J., Knox, R.E., Noakesfix, K., Allan, A., Eld, T., Kreizman, C., Brittain, K., McNee, S (2008). "Hype Cycle for Governance, Risk and Compliance Technologies, 2008.". Retrieved from Gartner, Inc.
26. Gangemi, A., Prisco, A., Sagri, M.T., Steve, G., Tiscornia, D. (2003). Some ontological tools to support legal regulatory compliance, with a case study. Workshop on Regulatory Ontologies and the Modeling of Complaint Regulations (WORM CoRe 2003), Catania, Italy, Springer LNCS Catania.
27. 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).
28. Skinner, C. (2008). Forensically evolving regulations. Retrieved from http://www.thefinanser.co.uk/2008/09/forensically-ev.html.
29. Hevner, A., March, S., Park J., Ram, S. (2004): "Design Science in Information Systems Research," MIS Quarterly, Vol. 28 No. 1, pp. 75-105.
30. 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.