COMPLIANCE MANAGEMENT AMONG CO-OPETING ACTORS

Abstract

This study obtains a set of guidelines with which IS designers can achieve regulatory compliance with data retention requirements. Previous work has explored how to assess compliance threats and to visualize the outcome of policies enforcement but has failed to address how regulatory compliance involves multiple agents seeking to optimize their individual payoffs. We propose a typology that acknowledges in the enterprise business model the return on investment of agents affected by the new controls. Such agents are assumed to be co-opeting, i.e. they gain by cooperating, even if they have different goals. Grounded in control theory and the technology acceptance model, our conceptual design and its implementation represent an economically viable way to align business, legal and IT requirements concerning regulatory compliance with data retention requirements.

1 Introduction

For the purposes of this study, compliance is "the act of adhering to, and the ability to demonstrate adherence to, mandated requirements resulting from contractual obligations and internal policies" (OCEG, 2009). Should these policies and standards not be observed, "compliance risk" arises, as described by the Basel Committee on Banking Supervision (2005). Compliance is part of a larger process known as Governance, Risk and Compliance (GRC), illustrated in figure 1, which includes the definition of policies (governance) and the mitigation of compliance risk (risk management). Recent financial scandals have shown the cost to enterprises of incidents that are due to a lack of compliance, which can be measured with a metric called Total Cost of Failure (Kahn and Blair, 2004). The Total Cost of Ownership of controls to ensure regulatory compliance can also be significantly high, and regulatory risk has topped the list of business threats perceived by managers (Economist Intelligence Unit, 2005), although some studies (e.g., IT Compliance Policy Group, 2008) report an increase in performance among those who excel in compliance management. Software can help enterprises respond to compliance needs, but it is up to the enterprise to define its requirements, knowing that one single and comprehensive GRC solution simply does not exist (McClean, 2009).

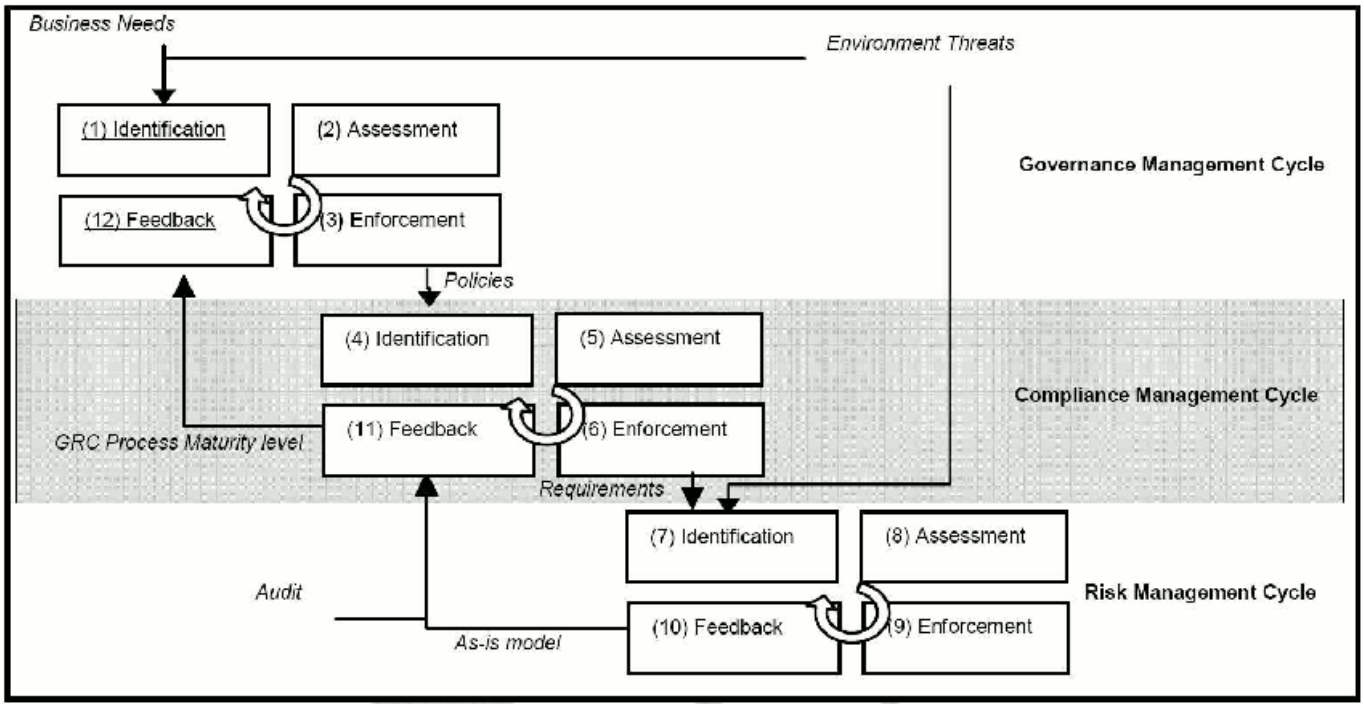

Figure 1: The IT GRC process

The remainder of the paper focuses on regulatory requirements concerning data retention for multinational companies in the financial sector. We believe the problem of data retention can be classed as "wicked" (Rittel and Webber, 1973) when an enterprise deals with different businesses in different countries and so must comply with multiple regulations with ambiguous, constantly evolving and sometime conflicting requirements. For example, a Swiss bank may have to "preserve for a period of not less than 3 years, the first two years in an accessible place […,] originals of all communications received and copies of all communications sent by such member, broker or dealer (including inter-office memoranda and communications) relating to his business as such" (Security Exchange Commission, 1934), yet the same Swiss bank has also to comply with Swiss regulations protecting employees' privacy.

Two main streams of research have addressed the GRC process. The first deals with the first three steps of the security management decision process proposed by Straub and Welke (1998)—that is, risk identification, risk analysis

and options analysis—which have the goal of achieving compliance by design. Among the large set of papers in this field we refer here only to Giblin et al. (2006), who proposed a solution to pass from enterprise policies to formal requirements for the IT architecture epxressed in UML, and to Jureta et al. (2010)'s theory of regulatory compliance for requirements engineering. We also acknowledge the IT solutions on the market, as described by Butler and McGovern (2009). With this stream of research, all stakeholders' requirements are formalized in order to minimize further adaptations and to achieve compliance by design, so the cost of controls is reduced. This approach recalls the theoretical claim of the property rights approach (Hart and Moore, 1990). The second stream of research deals with the last two steps of the process. We recall the work of Hoffman et al. (2009) for compliance checking and Bellamy et al. (2007) for compliance visualization and acknowledge a large set of IT solutions on the market for automatic control, for which we refer to Rasmussen (2006) for a rough classification. With this stream of research, a system is created to collect automatically all users' actions and perform data mining for compliance verification. According to transaction cost theory (Williamson, 2002), the cost of formalization declines at the requirement level and the quality of the process that is controlled increases.

We grounded our assessments in practice by performing a four-month full-time internship in the IT compliance team of a major financial institution headquartered in Switzerland. To define the controls and rules required, the compliance officer is expected to have a clear understanding of the domains of law, business and information technology (IT). From our experience, we believe that the existing research has missed three major issues:

- We lack a design theory for IT GRC that explains what happens among the multiple entities involved. The compliance situation appears to us to be one wherein all actors gain by cooperating, even if they have different goals. This combination of cooperation and competition can be called co-opetition (Nalebuff and Branderburger, 1998). For example, the legal department might be informed that a new regulation requires data to be retained for five years, which involves new investments for the IT department in terms of data storage systems and negatively impacts the business.

- The "risk" in business management is often seen as a requirement that has a risk, rather than one that also has a return on investment. The decision to comply with a regulation should be seen as an option with a cost and expected profits in the future, rather than only as a cost. In our example, the cost of simply storing data adds new cost whereas it does not bring any competitive advantage for the firm. Yet storing data could create value to the company if properly done.

- Compliance is a strategic issue, which rarely represented in the business model and almost never seen as a question of alignment. Since compliance is perceived by many enterprises as a strategic threat, the alignment among the business, IT, and the law should include the enterprise business model devised to avoid most compliance risk and reduce the number of required process controls. In our example, data management could be seen as an extension of an existing data management system for knowledge management, which would combine required controls with a return on investment over time for the company.

Accordingly, our research question is:

How can information systems be designed for sustainable data retention for regulatory compliance among co-opeting agents in multinational financial institutions?

2 Proposed Methodology

Design science creates and evaluates IT artefacts intended to solve organizational problems (Hevner et al., 2004, p. 7). Thus, the process we suggest starts with an organizational problem and ends with the evaluation of an artefact. Jones and Gregor (2008) go beyond the assumption concerning the advantages of a rigorous process to suggest that design research should deliver a theory at the end that extends boundaries beyond the context for which the artefact was developed.

Our starting point is a process with six steps (Peffers et al., 2007, p. 54): identify the problem and motivate, define the objective of a solution, design and develop, demonstrate, evaluate, and communicate. This process is composed of iterative cycles and has four "entry points" such that the researcher can start at any step from 1 to 4, depending on the initial conditions. If a design researcher deals with wicked problems, then the four entry points can be seen as maturity levels of the same process. The research can move forward only if the evaluation stage of each maturity level does not falsify previous claims. The four entry points can be split into two exploratory and two explanatory phases (Holmström et al., 2009).

In figure 2 the gray arrows represent the flows, which go backward if the validation phase falsifies the previous results. The backward arrows refer to the three kinds of contribution (Locke and Golden-Biddle, 1997, p. 1043): incompleteness (link F1), inadequacy (link F2) and incommensurability (link F3).

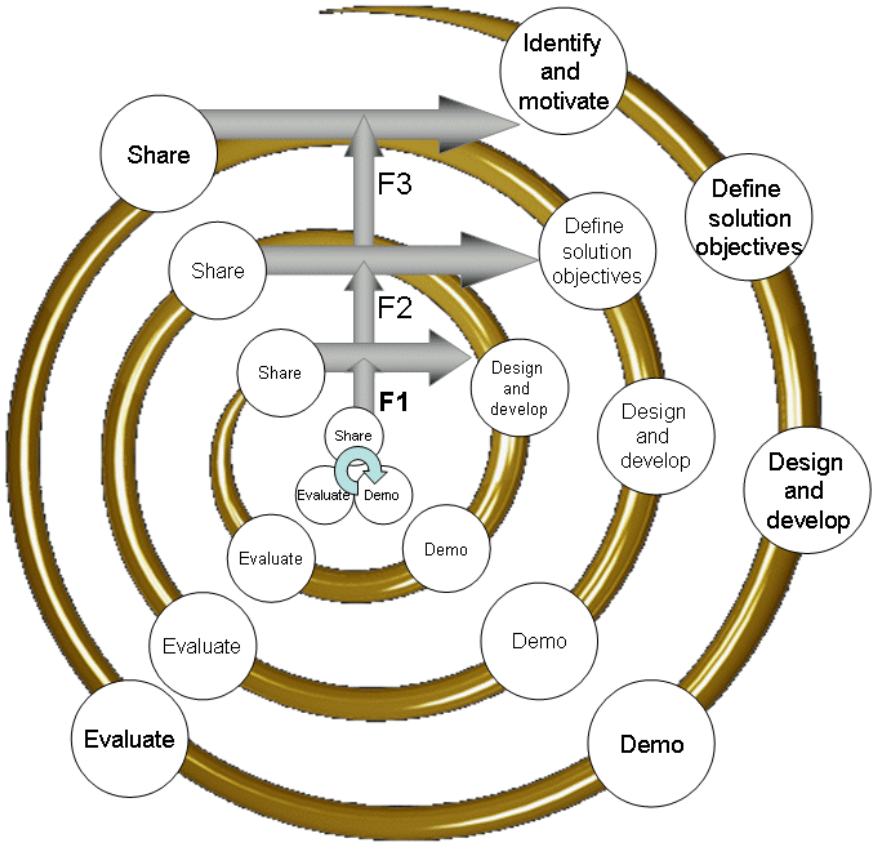

Figure 2: Proposed methodology

Table 1 shows how we applied the methodology to this study. The first task of the process is on the top of the spiral. The second step, the definitions of the objectives for a solution, was performed with the IT compliance officer. Once requirements were defined, an artefact was designed and developed to address the solution. In our case the artefact took the shape of a set of constructs (taxonomy for the control processes), a model (a Law-IT alignment framework), and a method (the IT GRC workflow). The evaluation of the artefact was descriptive, and it was presented as a master's thesis. Since the evaluation phase yielded positive results, we communicated the outcomes to the research community in two events (Bonazzi et al., 2008, Bonazzi and Pigneur, 2009).

Once the research community had been apprised of the outcomes and feedback had been collected, the PhD study began. More detailed problem analyses were performed, and we extended our scope to economically viable compliance systems among co-opeting companies, such as IT outsourcing and open innovation (a project done with a second financial institution). We developed a prototype to merge different viewpoints, and the evaluation of the business model came in the form of expert opinions from the financial institution. The outcomes were presented at an AIS workshop on co-opetition in open innovation (Bonazzi et al., 2009), and the article was selected for fast-tracking by the *International Journal of E-Services and Mobile Applications*.

Table 1: Timetable of the PhD study

Loop	Deadline	Artifact (s)	Evaluation	Communication
0	July 2008	Solution design: IT GRC Process; IT-Law alignment framework	Descriptive	ItAIS 2008; GRCIS 2009
1	September 2009	Software description: groupware for distributed requirement elicitation Business model for complliance among coopeting actors.	Testing	ItAIS 2009; IJESMA (forthcoming)
2	September 2010	Software description: privacy management application Prototype results with a small set of users (20)	Observational	BMMP 2010; Book chapter (forthcoming)
3	September 2011	Typology of design recommendations	Statistical (?)	n.a.

Since the results of the second evaluation were consistent with the previous results, we turned to development of a substantive theory. We decided to focus on a company outside the financial industry to avoid sample selection problems. Thus we worked with a major mobile handsets producer in the telecommunications business privacy management. We took the enterprise training course in software programming to develop a prototype to instantiate our theory of trust among co-opeting actors as the results of controls for contextual integrity (Nissembaum, 2004). We submitted the software to a competition for mobile application programmers and considered the feedback we received from the evaluating commission to be expert opinion. The business model considerations derived from the theory were presented at the IEEE workshop on business models for mobile platforms (Bonazzi et al., 2010). The detailed description of theory and prototype passed the first round of a call for chapter for a book on privacy protection measures and technologies in business organizations.

The fourth loop will be undertaken with the first financial company to test the theory quantitatively. We developed the theory in the form of a typology of control processes for data retention regulatory compliance with the primary goal of reducing compliance costs by sharing knowledge among stakeholders and by crowdsourcing the requirement engineering tasks.

3 Theoretical foundations

The theoretical foundation regarding decisions among different technologies can be found in the technology adoption model (TAM) proposed by Davis (1989) and recently extended by Venkatesh et al. (2003). In approach, compliance depends on the user's behavioral *intention to use* the control system. From the theory we derive two determinants that positively affect the behavioral intention: performance expectancy and effort expectancy.

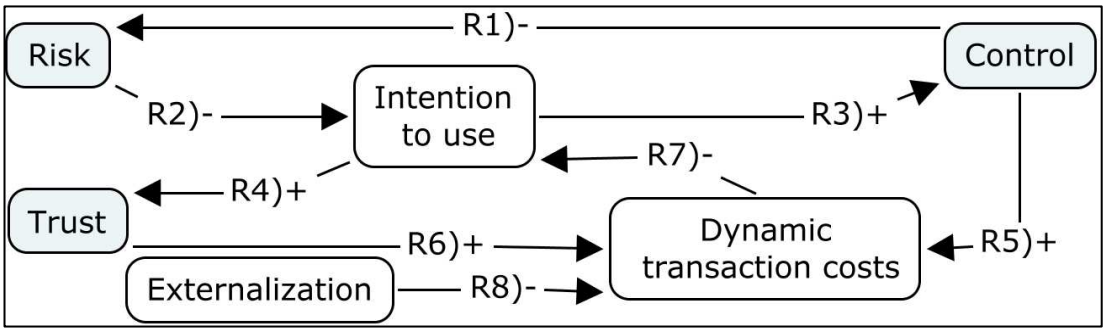

Figure 3: Conceptual model showing the mediating effect of intention to use on risk, trust and control

Control is defined by Das and Teng (2001) as the combination of three components: behavioral control (also known as process control), output control, and social control. A set of behavioral and output controls is obtained from formalizing social controls. According to Das and Teng, behavioral controls mitigate the relational risk (i.e., the risk that a partner will fail to honor its commitments), which affects the "goodwill trust," and output controls mitigate the performance risk, which has an influence on the "competence trust." Figure 3 shows these effects using the link R1. Goodwill trust and competence trust are similar to our definition of performance expectancy, so one could say that the relational risk and performance risk affect the performance expectancy, which has an influence on the intention to use the system (link R2). Gallivan and Depledge (2003) claim that information systems can reduce relational risk by monitoring co-opeting agents, which increases control (link R3) and knowledge share, which increases trust (link R4).

Dynamic transaction costs are the costs of persuading, negotiating and coordinating with, and teaching others (Langlois, 1992, p. 124). Both monitoring and collaborative uses of the system increase the dynamic transaction cost (link R5 and R6), which increases the required effort, which lowers the performance and the intention to use the system (link R7). Hence, link R8 shows how the co-opeting firms could decide to achieve sustainability by externalizing part of the required innovation and control activities (Chesbrough, 2003; Howe, 2006)

4 Current stage of the research

In this section we present how we intend to pass from the conceptual model (risk, trust and control) to the development of our artefact (risk, governance and compliance).

Our framework is inspired by Henderson and Venkatravam (1993, p. 476). We identify six types of stakeholder: three external to the company (a regulator that makes laws, a practitioners group that defines a framework, and an IT solution provider), and three within the company (a policy maker who defines enterprise policies, a compliance manager who assesses the internal control system, and an IS solution architect who elicits IS requirements for security engineering). Each decision is the result of the alignment of three constructs within the company (i.e., policies, internal control and security engineering IS requirement) under the constant changes among three contingencies: a set of data from the business unit (B.U.), whose attributes are derived from the business model proposed by Osterwalder et al. (2005); a set of legal updates (L.U.) on changes required in the policies, which can be retrieved from the existing regulatory content feeds, such as Complinet and LexisNexis; and a set of analyses of best

practices (B.P.) from one of the existing solutions benchmarks ("Hype-cycle" or "Wave"), performed by Gartner, Inc. and Forrester Research, Inc.

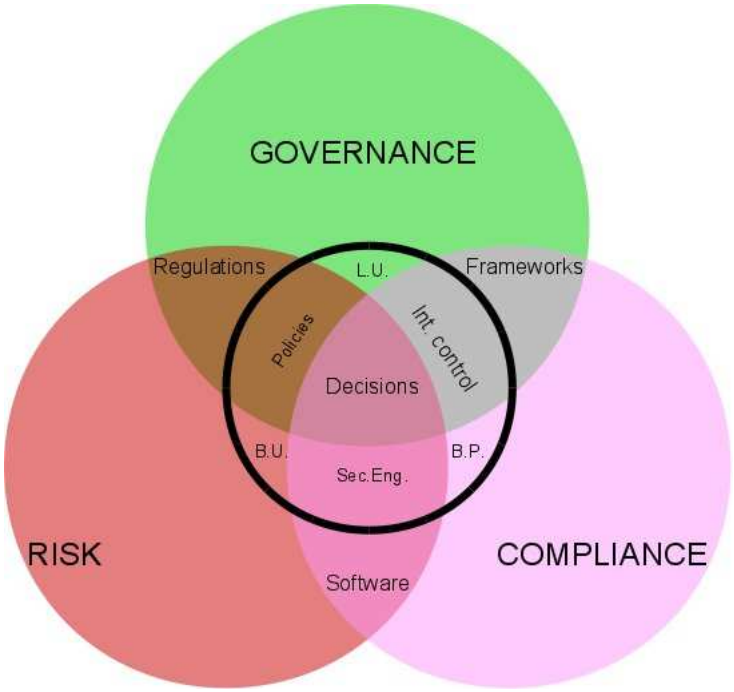

Figure 4: constructs of the system

The prototype has three main functions (figure 5): it retrieves and integrates information from three contingencies (business unit, legal update and best practices) and three internal constructs (security engineering, internal control and policies) by means of our taxonomy; it supports the monitoring decisions by presenting all data in a graphic format and by allowing the requirements to be enforced to be exported in an XML format; and it supports knowledge sharing and conflict resolution among stakeholders by representing their different viewpoints and highlighting the disagreements that should be given high priority.

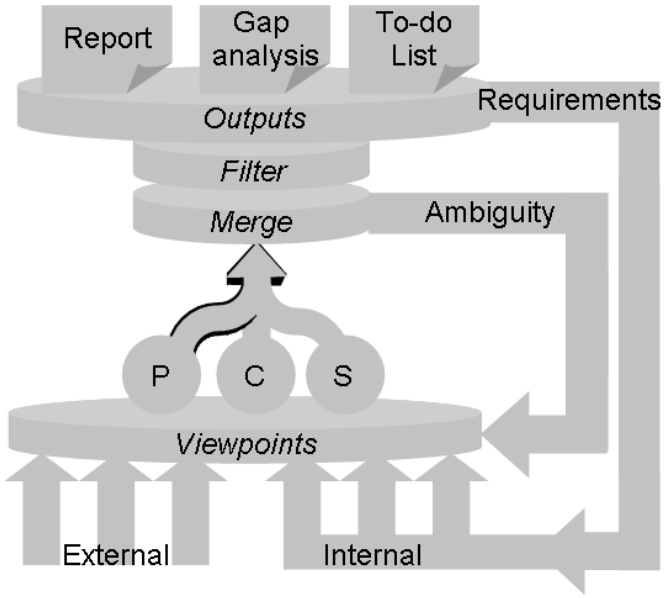

Figure 5: Data flow

To allow the artefact to be improved over time, we developed a set of ideal types of control actions (figure 6). From the COSO Enterprise Risk Management and the CobiT frameworks, we identify two core components for the internal control objects: the action to perform (verb) and the direct object of the action. In this sense "store" is a proactive action since it is triggered by an event at the moment it occurs. Our approach extends the idea of hierarchy mentioned by Cheng et al. (2008) such that, for example, "store mail" is a subset of "store communication data." this process allows for the creation of new control actions as combinations of verbs and direct objects and addresses the discrepancy of granularity between different regulations. Control activities could lead to economic returns as a consequence of increased operational quality, as suggested by the IT Policy Compliance Group (2008).

Figure 6: Verbs (left side of the figure) and direct objects of the verbs (right side of the figure)

In our groupware each construct is operationalized by means of a table, and each decision is a tuple of business unit, goal, control action and IT resource associated with the ID of the user and the user's degree of confidence in his or her decision (high, medium, low). Figure 7 shows a dashboard of the prototype.

4.1 Testable propositions

From the theoretical foundations, we derived our propositions to address the research question.

Our groupware to crowdsource the requirement engineering for regulatory compliance with data retention requirements is meant to reduce compliance costs while allowing knowledge sharing of compliance risk management policies among actors, ranked accordingly to their return on investment. Hence:

P1: A tool that decentralizes requirements reduces the compliance cost of adaptation.

Our business model is meant to create value for all stakeholders involved by aligning their interests and by reducing compliance risk. Therefore:

P2: Reducing compliance risk can add value to stakeholders because it reduces the number of control required.

We tested our typology by adopting it to model regulations from seven laws that affect IT. We obtained nine control actions, one of which is presented using a fictional scenario inspired from a real case. The SEC Rule 34 presented in table 2 is a regulation that requires storing communications. We estimated the compliance risk at $4.5 million. "Store Communication" is a control action similar to O'Grady's (2004) "Archive/Backup" service. This action is composed of the proactive verb *STORE* and the object *COMMUNICATION*, the latter of which is composed of financial communication, mail communication, chat communication, and SMS data. The conflict-resolution strategy privileges risk avoidance over cost savings and states that the control action with higher values should be chosen. The operational impact is estimated at $2000/GB, using Murphy's (2007) assessment of avoided e-discovery cost in a legal litigation. "Store communication" implements a storing system tool.

Communication archiving is an IT solution used to monitor data channels and to store indexed data. Its estimated Total Cost of Ownership (TCO) is $3 million as a fixed cost plus $50,000 every following year. The lead time to implement the solution is six months. To test the flexibility of our typology, we suppose a legal update for a new regulation that requires storing e-mail for five years. The company can choose simply to set the "time" parameter of the "store communication" control action from three years to five, but this solution would then store all communications, increasing costs beyond what was necessary to comply. Therefore, the company might decide to expand the list of control actions by adding "store e-mail," which implements the same IT solution as "store

communication" but, since the conflict resolution strategy is "maximize," the e-mail will be stored for five years, whereas the rest of the communications will be stored for only three years.

Table 2: Implementation of control actions to model laws impacting IT data retention

Verb	Object	Regulation	IT Solution
ON-GOING MONITOR	Employees activities	USA Patriot Act, Section 235	E-mail monitoring
ON-GOING MONITOR	Financial transactions	FINRA Notice to Members, April 2007	Payment filtering
ASSURE	Software effectiveness	USA Patriot Act, Section 352	Static Analysis Software
ASSURE	Internal Control	SOX 404	Data Loss Prevention
PROTECT	Customer Data	Gramm-Leach-Billey Act (Sec.501); EU Data Protection (art. 25); HIPAA 164.306;	Risk Prevention Tools
REPORT	Customer Activities	USA Patriot Act, Section 319	Transactions report
REPORT	Financial Activities	EU AMD, Point 9	Transactions report
STORE	Communications	FRCP, Rule 34	Comm.archiving
STORE	Customer Data	HIPAA, 164.528	Data Loss Prevention

6 References

Basel Committee on Banking Supervision, 2005. *Compliance and the compliance function in banks*, Basel Committee on Banking Supervision.

Bellamy, R. K. E., Erickson, T., Fuller, B., Kellogg, W. A., Rosenbaum, R., Thomas, J. C., & Wolf, T. V. (2007). Seeing is believing: Designing visualizations for managing risk and compliance. *IBM Systems Journal*, 46(2), 205-218.

Bonazzi, R., Fritscher, B., & Pigneur, Y. (2010). Business Model Considerations for Privacy Protection in a Mobile Location Based Context. In *Business Models for Mobile Platforms (BMMP) Proceedings*. Presented at the ICIN 2010, Berlin.

Bonazzi, R., Hussami, L., Bienz, P., & Pigneur, Y. (2009). Respecting the Deal: How to Manage Co-opetitive Actors in Open Innovation. In *Management of the Interconnected World*. Springer.

Bonazzi, R., Hussami, L., & Pigneur, Y. (2008). Compliance management is becoming a major issue in IS design. In D'Atri, A. & Saccà, D. (eds.), *Information Systems: People, Organizations, Institutions, and Technologies*. Springer.

Bonazzi, R., & Pigneur, Y. (2009). Compliance Management in Multi-actor Contexts. In *GRCIS09 Proceedings*. Presented at the *CAISE 2009*, Amsterdam. Retrieved from http://ceur-ws.org/Vol-459/paper7.pdf

Butler, T., & McGovern, D., 2009. A conceptual model and IS framework for the design and adoption of environmental compliance management systems. *Information Systems Frontiers*, 1–15.

Cheng, C.P. et al., 2008. Regulation Retrieval Using Industry Specific Taxonomies. *Artificial Intelligence and Law*, 16(3), 277-303.

Chesbrough, H. W. , 2003. The era of open innovation. *MIT Sloan Management Review*, 44(3), 35-41.

Economist Intelligence Unit, 2005. *Regulatory Risk: Trends and Strategies for the CRO*, Report from Economist Intelligence Unit.

Gallivan, M. J., & Depledge, G., 2003. Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, 13(2), 159–190.

Giblin, C., Muller, S., & Pfitzmann, B., 2006. From regulatory policies to event monitoring rules: Towards model driven compliance automation.

IBM Research Report. Zurich Research Laboratory.

Jones, D., & Gregor, S., 2008. The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, 8(5), 312-325.

Hart, O., & Moore, J., 1990. Property Rights and the Nature of the Firm. *Journal of political economy*, 98(6), 1119-1158.

Henderson, J.C. & Venkatraman, N., 1993. Strategic alignment: Leveraging information technology for transforming organizations. *IBM systems journal*, 32(1), 4-16.

Hevner, A. R., March, S. T., Park, J., & Ram, S., 2004. Design science in information systems research. *Management Information Systems Quarterly*, 28(1), 75–106.

Holmström, J., Ketokivi, M. & Hameri, A.P., 2009. Bridging Practice and Theory: A Design Science Approach. *Decision Sciences*, 40(1), 65-87.

Howe, J., 2006. The Rise of Crowdsourcing. *Wired*. Retrieved from http://www.wired.com/wired/archive/14.06/crowds.html.

IT Policy Compliance Group, 2008. *Annual Report: IT Governance, Risk and Compliance – Improving Business Results and Mitigating Financial Risk*, Report from T Policy Compliance Group.

Jureta, I., Siena, A., Mylopoulos, J., Perini, A., & Susi, A., 2010. Theory of Regulatory Compliance for Requirements Engineering. Retrieved from http://arxiv.org/pdf/1002.3711

Kahn, R., & Blair, B. T., 2004. *Information Nation: Seven Keys to Information Management Compliance*. Aiim International.

Locke, K. & Golden-Biddle, K., 1997. Constructing opportunities for contribution: Structuring intertextual coherence and" problematizing" in organizational studies. *Academy of Management Journal*, 1023-1062.

McClean, C., 2009. *The GRC Technology Puzzle: Getting All The Pieces To Fit*, Report from Forrester Research, Inc.

Murphy, B., 2007. *eDiscovery Best Practices,* Report from Forrester Research, Inc.

Nalebuff, B. & Brandenburger, A., 1997. Co-opetition: Competitive and cooperative business strategies for the digital economy. *Strategy & Leadership*, 25(6), 28-35.

Nissenbaum, H., 2004. Privacy as Contextual Integrity. *Washington Law Review*, 79(1), 101-139

O'Grady, S., 2004. *SOA Meets Compliance: Compliance Oriented Achitecture* (pp. 1-13). Red Monk. Retrieved from http://redmonk.com/public/COA_Final.pdf

Open Compliance & Ethics Group (OECG) , 2009. *Red Book 2.0 (GRC Capability Model).* Retrieved from http://www.oceg.org/

Osterwalder, A., Pigneur, Y., & Tucci, C. L., 2005. Clarifying business models: Origins, present, and future of the concept. *Communications of the association for Information Systems*, *16*(1), 1-25.

Peffers, K. et al., 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45-77.

Rasmussen, M., 2006. *Overcoming Risk And Compliance Myopia*, Report from Forrester Research, Inc.

Rittel, H., & Webber, M. 1973. Dilemmas in a General Theory of Planning, *Policy Sciences*, 4(2), 155–169

Security Exchange Commission, 1934. *Securities Exchange Act of 1934, Rule 17a-4*. Retrieved from http://taft.law.uc.edu/CCL/34ActRls/rule17a-4.html

Straub, D. W., & Welke, R. J., 1998. Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469.

Williamson, O.E. (2002). The theory of the firm as governance structure: From choice to contract. *The Journal of Economic Perspectives*, 16(3), 171-195.

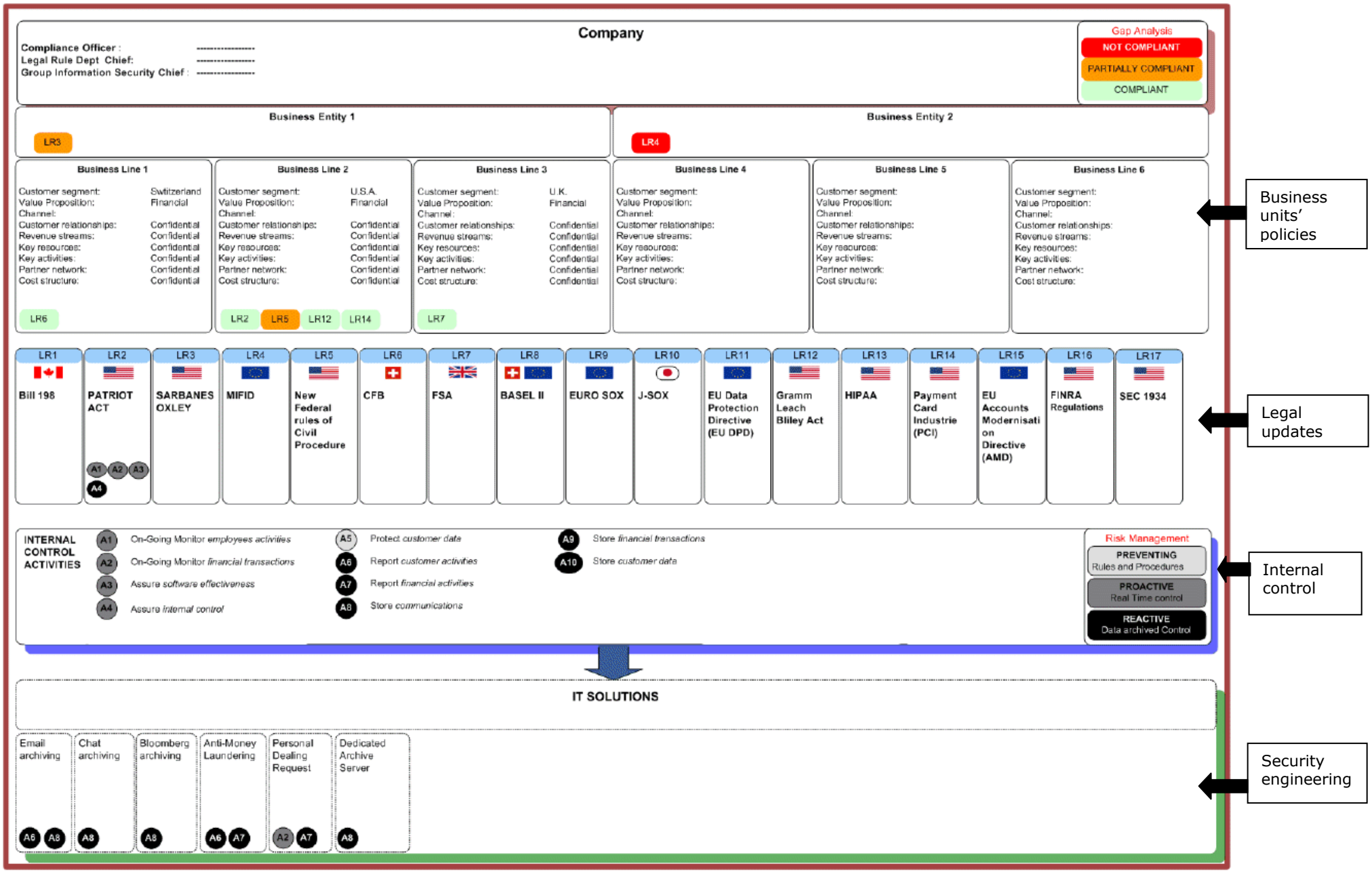

Figure 7: the dashboard of the first prototype we developed