Year : 2012

DESIGNING A COMPLIANCE SUPPORT SYSTEM

BONAZZI Riccardo

UNIL | Université de Lausanne

FACULTÉ DES HAUTES ÉTUDES COMMERCIALES

DÉPARTEMENT DES SYSTÈMES D'INFORMATION

DESIGNING A COMPLIANCE SUPPORT SYSTEM

THÈSE DE DOCTORAT

présentée à la

Faculté des Hautes Etudes Commerciales
de l'Université de Lausanne

pour l'obtention du grade de
Docteur en Systèmes d'Information

par

Riccardo BONAZZI

Directeur de thèse
Prof. Yves Pigneur

Jury

Prof. Daniel Oyon, Président
Prof. Ari-Pekka Hameri, expert interne
Prof. Alain Wegmann, expert externe
Prof. Maung Sein, expert externe
Prof. Richard Welke, expert externe

LAUSANNE
2011

IMPRIMATUR

Sans se prononcer sur les opinions de l'auteur, la Faculté des hautes études commerciales de l'Université de Lausanne autorise l'impression de la thèse de Monsieur Riccardo BONAZZI, titulaire d'un Bachelor en Ingénierie de Gestion de l'Université de Bologna, titulaire d'un master en Business Information Systems de l'Université de Lausanne, en vue de l'obtention du grade de docteur en Systèmes d'information.

La thèse est intitulée :

DESIGNING A COMPLIANCE SUPPORT SYSTEM

Lausanne, le 31 Novembre 2011

Le doyen

Daniel Oyon

Doctoral committee

Prof. Yves PIGNEUR
Faculty of Business and Economics (HEC), University of Lausanne
Director of thesis

Prof. Ari-Pekka HAMERI
Faculty of Business and Economics (HEC), University of Lausanne
Internal member of the doctoral committee

Prof. Maung SEIN
Faculty of Economics and Social Sciences, University of Agder
External member of the doctoral committee

Prof. Alain WEGMANN
School of Computer and Communication Sciences, EPFL
External member of the doctoral committee

Prof. Richard WELKE
Robinson College of Business, Georgia State University
External member of the doctoral committee

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Riccardo BONAZZI

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation.

Signature : Yves Pigneur Date : 18 novembre 2011

Prof. Yves PIGNEUR
Directeur de thèse

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

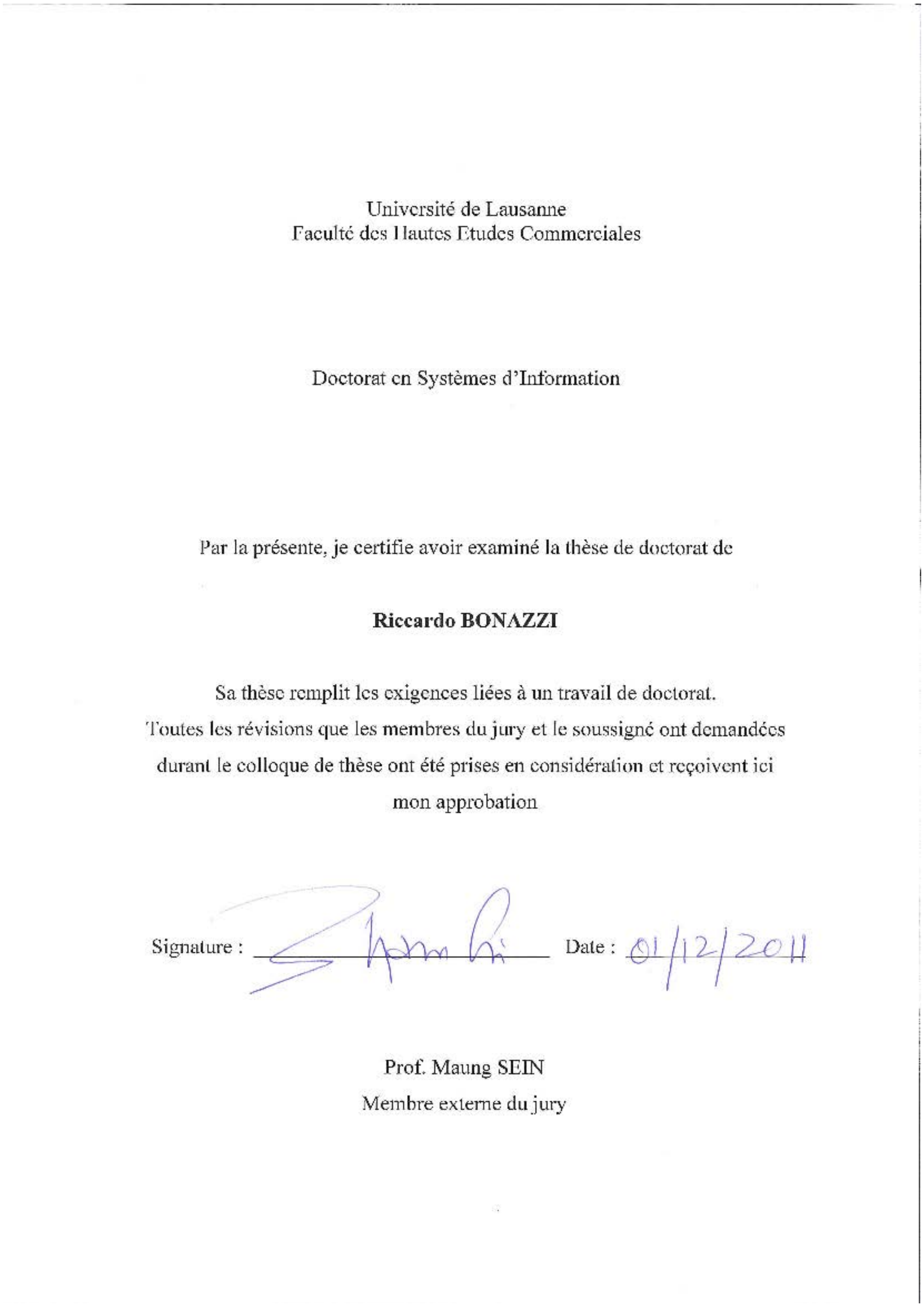
Par la présente, je certifie avoir examiné la thèse de doctorat de

Riccardo BONAZZI

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées
durant le colloque de thèse ont été prises en considération et reçoivent ici
mon approbation.

Signature : ___________________________ Date : ___26.11.2011_________

Prof. Ari-Pekka HAMERI
Membre interne du jury



Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

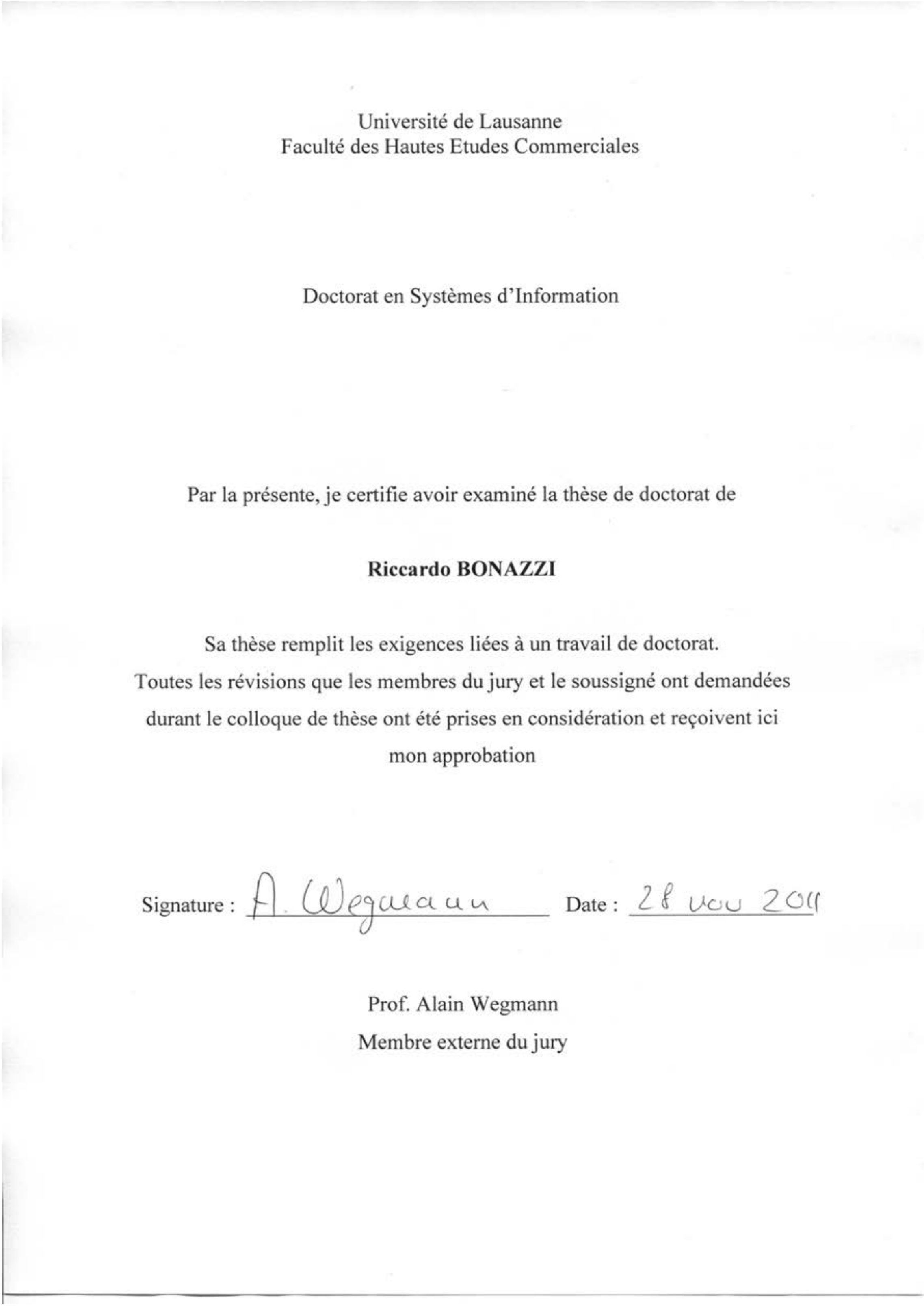
Par la présente, je certifie avoir examiné la thèse de doctorat de

Riccardo BONAZZI

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées
durant le colloque de thèse ont été prises en considération et reçoivent ici
mon approbation

Signature : ______________ Date : 01/12/2011

Prof. Maung SEIN
Membre externe du jury



Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Riccardo BONAZZI

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation

Signature : A. Wegmann Date : 28 nov 2011

Prof. Alain Wegmann
Membre externe du jury

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Riccardo BONAZZI

Sa thèse remplit les exigences liées à un travail de doctorat. Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation

Signature : Welke Date : 30/NOV/2011

Prof. Richard WELKE
Membre externe du jury

I don’t know how to not have fun.

And I am going to keep having fun every day I have left

(R. Pausch)

Abstract

This research addresses the compliance burden of most firms that operate in markets with a large number of regulations. It does so by proposing a solution that iteratively searches for conformity. I propose a system that collects the viewpoints of the agents involved; these viewpoints take the form of control actions. Whenever possible, this system codes control actions using taxonomies derived from existing literature. Then, the system merges the agents' viewpoints and tests their combined influences over the agents' perceived payoff. The result of these tests is a quantitative representation of the agents' aggregated view of the context in which they are situated (grounded theory). By assigning a preferred course of action to each specific context the system obtains a set of patterns. Such patterns can be reused among practitioners. In addition, scholars can test them as a form of mid-level theory (i.e., a typology). This thesis offers a greater understanding of the importance of making a distinction between compliance and conformity, based on the assumption that the regulated agents are, at the same time. I propose a solution that extends the existing body of literature on information system compliance management in a rigorous and relevant way.

The outcome of this work is the result of four main iterations that were performed by working with practitioners in companies. These iterations helped me to link the theoretical problem to practical issues and I am thankful to the companies that allowed to me work with them. As a consequence of the learning effect that each had on me the chapters of this thesis are presented in different styles. To include such incoherences is a deliberate choice of mine, revealing the learning process that I followed in carrying out this research.

Nevertheless, I have decided to present the result of these iterations in a linear way in the first chapter, which describes the overall problem, the chosen methodology, the theoretical model used and the results obtained. The first chapter concludes by listing further works that can be carried out.

Most chapters in this thesis are derived from articles that have already passed at least one round of reviews and have been published in conference proceeding, or as book chapters or and journal articles. In the following pages I acknowledge the path that I have been following to obtain these results and the name of those, who helped me in these years.

Acknowledgements

I have to confess that during my PhD I had much more fun than I would have expected. So if you are looking for long descriptions of pain and sacrifice in this text, I am sorry to disappoint you. According to game design principles, fun is achieved when a balance between challenges and rewards is achieved. Too many challenges becomes frustrating, whereas too many rewards becomes annoying. Reading academic articles is fun because it gives one the tools to solve a challenge and to attain a reward, whilst at the same time, opening the way to a new set of problems. The resulting journey is a never-ending path, which I feel that I have just embarked on.

In my journey I have been not alone and I would like to list here the names of those with whom I had the pleasure of working. If your name does not appear here it might be because I have decided to send you a copy of this thesis with a handwritten note by way of thanks, or I might not be aware of your interest in this field when I started writing this thesis. Following publication of this thesis, I welcome discussion with those in this field with whom I have not made contact yet.

For the first chapter I would like to thank Professors Ari-Pekka Hameri, Maung Sein, Alain Wegmann and Richard Welke, who have helped me to make many improvements. Previous versions of the first chapter were presented at the Doctoral Consortium of the European and of the Australasian Conferences in Information Systems. I would like to thank Professors Shirley Gregor, Ulrike Schultze and Ron Weber for the useful comments that I received on those occasions. The methodology section was inspired by a paper written for the course delivered by Prof. Mikko Ketokivi "Scholarship in organization science". It was further improved whilst studying for the course delivered by Prof. Matthias Finger on "Qualitative Methods".

With respect to the second chapter I would like to thank Walid Drira and Lotfi Hussami, who coached me during my internship, and Prof. Yves Pigneur, whose support was greatly helpful in converting my master's thesis into a publishable paper.

The first version of the third chapter was written whilst studying for Prof. Johan Roos's course "Engaged Scholarship". I would like to thank Prof. Yao-Hua Tan for his useful advice concerning potential applications in the World Customs Organization (WCO) of the proposed dashboard.

Most of my contributions to the fourth chapter were made during ACIS 2010, when I met Nicolas Racz. At that time, Nicolas was working at the Vienna University of Technology and I found the experience of co-authoring a paper without seeing each other to be very enriching.

The fifth chapter was written during M. Jay Galbraith's ”Organization Design for Innovation, Technology and Product Development” course and that delivered by Prof. Allan Afuah's ”Theory Development in Corporate Strategy and Technology Innovation”. A special thanks goes to Andrea Zeller and Gijs van den Heuvel for their useful advice.

The sixth chapter is an extension of the master's thesis submitted by Charlotte Ceccaroli. I would like to thank Prof. Stephanie Missonier, who helped me translate the creative mess in my mind into a coherent story on paper.

With respect to the seventh chapter I acknowledge the useful talks, that I had with Prof. Dimitris Chorafas during his course on ”Integrated Risk Management”.

When writing the eighth chapter, I was deeply inspired by Prof. Ron Sanchez's ”Managerial Decision Making” course, as well as that delivered by Prof. Phil Bromiley on ”Strategic decision-making processes within organizations”. The development of privacy management software gave me the opportunity to work with Simon Garniere from Deloitte AG and with Zhan Liu, whom I admire for being such a hard worker and who I thank for reminding me to sometimes take a break.

The ninth chapter is a consequence of the many interesting conversations I had with Boris Fritscher. Much of the test design is derived from the paper I wrote as part of the course on ”Data Analysis in Management Research” offered by Prof. Andrew King. Jialu Shan and Maria Dobrinas helped me a lot during the data analysis.

The tenth chapter describes an on-going project supported by the University of Lausanne. This project began with my discussions with Prof. Dominique Jaccard about an idea that Emmanuel Fernandes and I had back in 2008.

The eleventh chapter describes an on-going project with the Nokia Research Center. A first draft of the theoretical model was developed following the advice of Samuel Bendahan and Philippe Jacquart during the course on ”Structural Equation Modeling”.

Contents

List of Figures

Part I

Part 1: Designing a Compliance Support System

Chapter 1

Introducing the elements of the problem

1.1 Background and definition

This first chapter provides a general overview of the problem addressed in this thesis and how I intend to address it.

1.1.1 Compliance

In this study, compliance is defined as " the act of adhering to, and the ability to demonstrate adherence to, mandated requirements resulting from contractual obligations and internal policies " [99]. Should these policies and standards not be observed, " compliance risk " arises, as described by the Basel Committee on Banking Supervision [174]. Therefore, compliance is part of a larger process known as Governance, Risk and Compliance (GRC), which includes the definition of policies (governance) and the mitigation of compliance risk (risk management). However, compliance is a complex issue.

1.1.2 Compliance costs

First, there is the cost of non-complying. Recent financial scandals have shown the costs to an enterprise of incidents that arise from a failure to comply. The cost of non-compliance can be measured using a metric called Total Cost of Failure [128]. On the other hand, in recent years the Total Cost of Ownership of controls for regulatory compliance has been shown to be potentially high. The regulatory risk has even topped the list of business threats perceived by managers [236],although some studies [98] report an increase in performance for those who excel in compliance management. Software exists to respond to different compliance needs [154], but it is up to the enterprise to define its requirements, knowing that a single and comprehensive GRC solution does not exist.

1.1.3 Co-opetition

Second, the relationship between those being regulated and those who regulate (regulators, is simultaneously cooperative (both have an interest in following the regulations) and competitive (they might have conflicting goals)[16]. I define this relationship between cooperation and competition as co-opetition [163], which I measure as agents' perceived lack of fit with their goals.

1.1.4 Ambiguous and constantly evolving compliance requirements

Enterprises that deal with different businesses in different countries have to comply with multiple regulations; these tend to be ambiguous, constantly evolving and sometimes conflicting. For example, the USA Patriot Act is an American law that requires Swiss banks in the United States to share data about their customers with American authorities to prevent terrorism. The Swiss banks must also comply with Swiss regulations concerning customers' privacy.

1.1.5 Compliance requirements for data storage and retention

The remainder of this chapter focuses on regulatory requirements relating to information systems for data retention and protection for firms that are subject to a large set of regulations. This type of problem involves making decisions on the data to be collected, how it should be stored, who should be able to access it, how much time it would take to retrieve it and when it should be deleted. For these tasks, a trade-off among regulatory requirements has to be found. Different regulations can request that some data be stored (e.g., information among traders concerning the business itself), whereas other regulations stipulate that some data cannot be stored without the client's consent (i.e. privacy issues). Moreover, some regulations require data to be stored for at least five years and to be ready for retrieval within 30 days. Some regulations request that data be deleted after a certain amount of time and be stored using encryption.

I believe such a problem can be classed as "wicked" [109]. To address such a problem, an appropriate research approach is design science. This is the approach followed in this thesis.

1.2 Research questions

The purpose of this thesis is to identify a system that is easy to use and adapt in response to a large set of constantly evolving regulations. Accordingly, this thesis aims to gain a better of understanding how to design an information system for regulatory compliance among multiple agents who are subject to the law. The research question can be stated as follows:

How to design easy-to-use and easy-to-adapt information systems for data retention regulatory compliance among co-opeting agents subjected to a large number of constantly evolving regulations?

I begin by addressing the underlying assumption of most research in IS compliance management with regard to regulated agents. These agents are assumed either to be willing to be regulated or are in need of being strictly controlled. I then go on to explore what could be achieved if one assumes that regulated agents are, at the same time, competing and cooperating. For example, they could be competing for access to limited resources (e.g., business units trying to get a greater part of the corporate budget), whist at the same time cooperating to show evidence of compliance (e.g., business units are supposed to share data in order to allow effective internal control).

Therefore, the first research sub-question of this thesis seeks a new problem definition. Its underlying assumption is that there are inconsistent goals among regulated agents within a firm. Following on from this, a the cause for inconsistency is sought.

Research sub-question 1: How can a relationship between the regulator and regulated agents be modeled in order to involve both cooperation and competition?

The next step is to propose a viable solution. In order to be accepted by technology-savvy and business-oriented agents the solution must address both their concerns and legal requirements. The introduction of the concept of a pattern is intended as a solution to a recurring problem. The creation of such a pattern for control can be considered as the development of an artifact, as required by design science. Hence, I aim to obtain a collection of patterns, which I define as a typology. According to Doty and Glick [70], typologies can be considered as a form of mid-range theory, which would allow relevance and rigor to be correctly combined in the results obtained. Thus, the second research sub-question is as follows:

Research sub-question 2: What are the components of a control pattern among agents with inconsistent goals?

The constant evolution of regulation requires a system that is easy to adapt. In this thesis I follow the guidelines put forward by Gregor and Jones [96] in order the concepts of artifact mutability and kernel theories to the description of my artifact. The artifact's mutability is defined thus: "degree of artifact change is encompassed by the theory" (p.332). The kernel theories are defined as "the underlying knowledge from the natural or social or design science that gives a basis and explaination for the design" (p.322).
To do so, I refer to Van Aken's [238] assessment of design science as delivering three outputs: an artifact, a set of guidelines to use that artifact and a set of guidelines to create it. I aim at addressing these points by answering the following research sub-question:

Research sub-question 3: How can one create new control patterns that are easy to use and to adapt?

The following paragraph seeks to explain how these three research sub-questions can be addressed.

1.2.1 Structure of this chapter

The following section presents the research approach used in this study. Section 1.4 presents the propositions that have driven the creation of the artifacts. In section 1.6 I present the articles already published and illustrate how they contribute to the overall theoretical framework proposed in this thesis. Finally, in section 1.7 I respond to the research question and its three sub-questions by using the propositions of the theoretical framework and describing the evidence presented in the published articles.

1.3 Research approach

This section presents the research approach used by linking it to design science in information systems and, more generally, to design science in management. The resulting methodology is illustrated in figure 1.1. The grey arrows in my model represent the flows that occur if the validation phase falsifies the previous results. This section refers to the different kinds of contribution listed by Locke and Golden-Biddle[146], which address incompleteness (F1), inadequacy (F2) or incommensurability (F3).

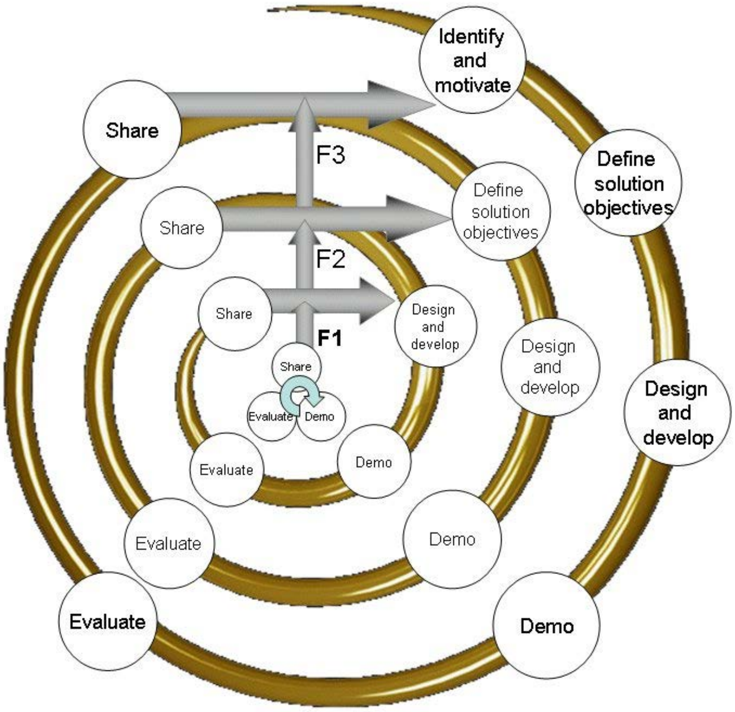


Figure 1.1: The chosen methodology)

1.3.1 An overview of the methodology

According to Hevner et al. [109], design science ”creates and evaluates IT artifacts intended to solve identified organizational problems”. The process suggested in this thesis starts with an organizational problem and ends with the evaluation of an artifact. Gregor and Jones [96] went beyond the assumption that a rigorous process extends certain advantages, suggesting that design research should deliver a theory that extends boundaries beyond the context for which the artifact was originally developed.

The starting point of this thesis is the process proposed by Peffers et al. [182], which has six steps: (1) Identify problem and motivate, (2) Define objective of a solution, (3) Design and Development, (4) Demonstration, (5) Evaluation and (6) Communication. Such a process is composed of iterative cycles and has four "entry points"; that is to say, the researcher can start at any step ranging from 1 to 4 depending on the initial conditions. If a design researcher deals with wicked problems, then the four entry points put forward by Peffers et al. [182] can be seen as a maturity level of the same process, something which can only be reversed if the evaluation stage falsifies previous claims.

A comparison can be made with a methodology that has been proposed in information systems. Action design research (ADR) [215] combines design research and action research to enlarge the focus of research to be placed on enterprises, particularly to help obtaining technological rigor and organizational relevance. The methodology has four interacting elements. The first two guiding principles for problem formulation concern (1) the need to find a balance between theory and practice. The building, intervention and evaluation phase (2) is guided by three principles, which require a close relationship between researchers and practitioners. The third element (3) is dedicated to reflection and learning and it should satisfy guided emergence. The last element (4) concerns generalization of the outcomes. It is my opinion that my methodology informs action design research because the two approaches already have much in common; that is to say, the idea of iteratively shifting from theory to practice and vice versa, and close ties to practitioners. Nevertheless, my framework has different points at which the generalization of outcomes occurs, in order to collect the feedback from peer-reviewers while the project is still ongoing.

Peffers et al.'s [182] entry points recall the four phases of the approach proposed by Holstrom et al. [113], which has two exploratory and two explanatory phases. At the end of each phase, I propose a generalization of outcomes and retain the names for the tasks adopted and used by Peffers et al. [182]. In the figure each iteration occupies a line that is associated with a phase put forward by Holstrom et al. [113].

Finally, the outcome of this thesis has been identified by some scholars as being similar to grounded theory; hence, I use the criteria put forward by Glaser and Strauss [92] to assess the quality of the theory presented in terms of a compliance support system:

- Fitness: my theory is meant to apply to design guidelines for information systems to ensure data retention and protection regulatory compliance. So far the proposed model has been confirmed both by practitioners who have implemented it and by scholars who have cited the published articles (for example the paper presented at ECIS 2011 by Wiesche et al. [255]) or have contributed to its development and extensions (for example the article presented in chapter 4 [192]).
- Understanding: the major contributions of this model are to give a unified view to the different aspects of compliance, and to (re)introduce the concept of return on investment as an important element in the decisions made by regulated agents.

– Generality: the compliance support system framework has been tested in different firms and different business domains.
– Control: the structural model is grounded in existing theories, and is associated with a measurement model that has been conceived to properly test causality.

1.3.2 Applying the methodology to obtain three artifacts

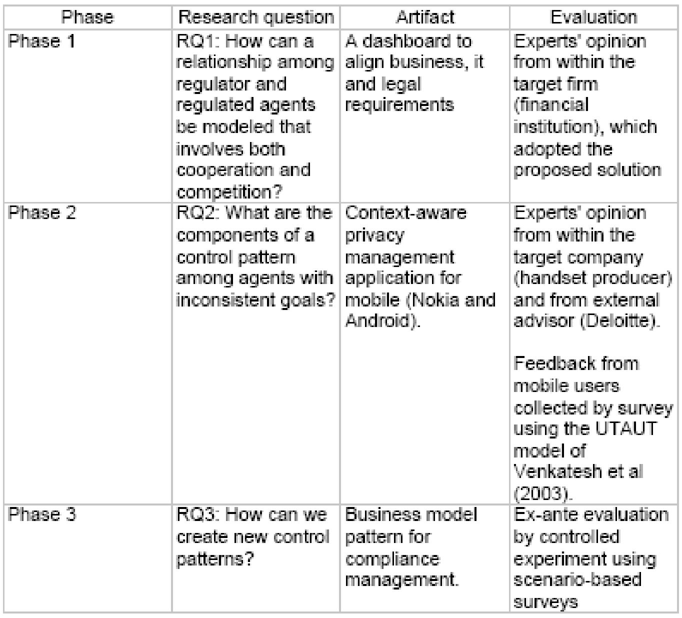
In figure 1.2 my methodology is instantiated by describing in detail how it iteratively advanced in this thesis.

Phase 0: Understanding the problem and developing the main assumption. The first task of the first loop of the spiral presented in figure 1.1 is the identification of the problem and its motivation. This was carried out as part of my master's thesis, by collecting articles on GRC and by meeting with experts from banks and other research centers. The second step, to define the objectives of a solution, was performed with the IT compliance officer in a financial institution. Once requirements were defined, it was possible to propose a method (the IT GRC workflow) that led the identification of the central assumption that regulated agents have partially conflicting goals and few incentives to conform to regulation.

Phase 1: Developing a dashboard to align business, IT and legal requirements. To address the first research sub-question, it was first necessary to identify the problem and motivate the interest of the research community. To address the first gap in the literature regarding how to design sustainable compliance management systems, I first designed a dashboard artifact that offers a simple view into compliance data. Requirements from business, IT and legal agents in the financial institution were collected to create a taxonomy of control actions that would allow the dashboard to evolve over time. This initial artifact enabled a better understanding of the kind of problem and the types of agents involved, adding a third dimension to the standard business-IT alignment effort. The way the dashboard was conceived allowed three entry points, or three contingencies. In so doing, it went beyond the traditional view of viewing regulation as the only driver of change.

Phase 2: Developing a context-aware privacy management application for mobile devices. The third phase develops a substantive theory to address the second research sub-question. Initially. it was decided to focus only on data retention for privacy management, as this was seen as another problem that relates to regulatory compliance in data management. This time, I worked with a major producer of mobile handsets within the telecommunication business, an industry that operates outside of the financial domain. Software was developed (i.e., a context-aware privacy management system) to assess the performance of a regulatory system that adapts itself according to the surrounding environment. The second artifact enabled a better understanding of the kind of solution being sought; however, it did not lead to a better understanding of how to generate the rules for my system. Previous security applications were technology-driven and omitted the behavioral side of human-computer interaction, mostly using simulations as a means of evaluation. This mobile application is a extension of previous work because it is built around a rationally bounded user and adapts to a dynamically changing context.

Phase 3: Designing a business model pattern for compliance management. The last iteration addresses the third research sub-question. The typology of control processes was quantitatively tested for data retention regulatory compliance, with a special interest in privacy management. The last artifact brought about an understanding of how to generate and assess different control solutions, as well as how to represent them in the form of business model patterns. Business model patterns extend the idea of business rules by adding key components, such as customer segment and return on investment.



Phase	Research question	Artifact	Evaluation
Phase 1	RQ1: How can a relationship among regulator and regulated agents be modeled that involves both cooperation and competition?	A dashboard to align business, it and legal requirements	Experts' opinion from within the target firm (financial institution), which adopted the proposed solution
Phase 2	RQ2: What are the components of a control pattern among agents with inconsistent goals?	Context-aware privacy management application for mobile (Nokia and Android).	Experts' opinion from within the target company (handset producer) and from external advisor (Deloitte). Feedback from mobile users collected by survey using the UTAUT model of Venkatesh et al (2003).
Phase 3	RQ3: How can we create new control patterns?	Business model pattern for compliance management.	Ex-ante evaluation by controlled experiment using scenario-based surveys

Figure 1.2: Link between research questions and artifacts

1.4 Theoretical model

This thesis aims to go beyond previous research by delivering an alternative view for IS compliance management. Two main streams of design research have addressed the Governance, Risk and Compliance process: (1) requirement engineering oriented and (2) business process oriented. In my view, compliance among agents is the result of a decision process. It is line with the decision process for security management proposed by Straub and Welke [230], which can be used to merge the two main research streams in GRC. A recent study of psychological drivers that enhance compliance has appeared in a recent issue of MISQ ([44]) ; however, it is not yet mainstream research. Another recent study used grounded theory to derive a set of enabling factors for GRC [255]. A theory that unites those four drivers has yet to be found.

This section present a model to address the research question posed by this thesis, together with its three sub-questions. Such a model was produced following the results of the analysis of the three cases. It is represented in figure 1.3.

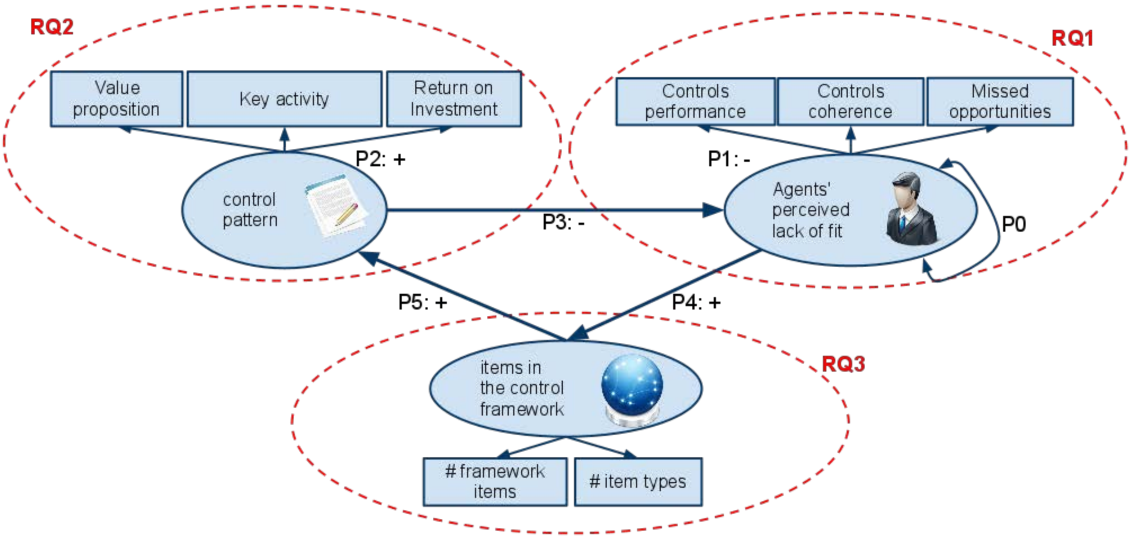


Figure 1.3: The proposed theory

Agents' lack of fit causes co-opetition. The following paragraph describes my initial assumption regarding the state of inconsistency among regulated agents' goals, which is measured using their perceived fit. This thesis aims to address this problem.

Agents' perceived lack of fit is caused by the misalignment of three dimensions. The first paragraph addresses the first research question and explains how it is measured by collecting agents' perceived control performance, control coherence and missed opportunities.

Control patterns reduce agents' perceived lack of fit. To solve this problem and to address the second research sub-question in the second paragraph, I propose to use a solution called control pattern,. This is presented in the third paragraph and extends the idea of business rules for process management.

A control framework allows adaptations when regulations change. Finally, the third paragraph addresses the third research sub-question. It deals with artifact mutability, which is defined here as the degree of artifact change encompassed by the theory. In order to face constantly evolving regulations, the fourth paragraph introduces the idea of a control framework. This framework is composed of the items inserted by regulated agents, which are then refined into control patterns.

1.4.1 Agents' lack of fit causes co-opetition

My initial assumption concerns the idea of fit among agents who are involved in designing a compliant information system. In order to maintain its existence in a specific context (i.e., viability), a firm must regulate, optimize and continuously improve its internal operations and must manage its relationships with external entities [17]. Such interactions appear in two basic ways: cooperation for the exchange of resources [104, 83] and competition to acquire/maintain customers [186] and resources [210]. In various business settings, firms compete and cooperate at the same time to achieve both advantages and viability. This hybrid form of strategy, which comprises simultaneous cooperation and competition, is labeled co-opetition in the strategy literature [32].

According to Colby and Kohlberg's [51] levels of moral perspective, agents can behave in three ways: deviance (to not respect the rules), conformity (to fully agree with the rules) or something in between, such as compliance (to respect the rules, even if one does not agree with them). By assuming inconsistency of goals among co-opeting agents, it implies that it is not enough to simply collect agents' requirements, since they are less likely to be totally true. However, one cannot simply control everything agents do, because most of their actions are driven by the intention to cooperate. To my knowledge, there is a gap in the GRC literature regarding the work carried out under the assumption of co-opetition; a gap which this thesis seeks to address. In the case of regulatory compliance, it can be assumed that a company needs to maximize the fit among conflicting dimensions such as business, IT and law, which for simplicity I associate here with three agents (one manager per dimension). The concept of co-opetition is then applied at the group level, with the fit among co-opeting agents not increasing per se without support. Thus, it is possible to state that the starting assumption is as follows:

P0: The lack of fit covariance among co-opeting agents does not decrease over time.

1.4.2 Agents' perceived lack of fit is caused by the misalignment of three dimensions

An important stream of research in GRC deals with the first three stages of the security management decision process put forward by Straub and Welke [230] - risk identification, risk analysis and options analysis - as it tries to achieve compliance by design. From among the large body of literature in this field, one can point to Giblin et al. [91], who proposed a solution for passing from enterprise policies to formal requirements, and to Jureta et al. [127]'s theory of regulatory compliance for requirements engineering. The existence of IT solutions on the market should also be acknowledged: these have been described by Butler and McGovern [39].

The general idea of such research is that once all stakeholder requirements are formalized, in order to minimize further adaptations and to achieve compliance by design, costs of controls are claimed to be reduced. The underlying assumption of this stream of research can be found in the large body of research work that is based around self-reinforcing contracts derived from information economics. The revelation theory states that, " any allocation rule obtained with a mechanism can be also implemented with a truthful direct mechanism " [21]. The problem of requirement engineering among co-opeting agents is that their declarations might not be truthful. The power of this approach is that it assumes that agents have an incentive to tell the truth if they are properly rewarded by the mechanism in place. This process works in two stages. In the first stage, each agent declares their true expectations and a contract among them is defined. In the second stage, the contract is executed and the agents' payoffs are fixed at a predetermined threshold (in other words, repayments are flat), which gives no incentive to lie about the outcome.

Once the mechanism is found, the challenge is to implement it by defining the agents' expectations. Starting from the definition put forward by Rosemann et al. [208], this thesis builds on the work of Wiesche et al. [255], who identified four value drivers for Information Systems Governance, Risk and Compliance: (1) control performance, whose objective is efficiency of auditing; (2) control coherence, whose objective is effectiveness of controls; (3) risk responsiveness, whose objective is the interpretation of weak signals; and (4) management resilience, whose objective is the achievement of rationales for actions. The lack of fit among agents is the result of the conflicting directions of regulatory requirements for control performance, technological requirements for control coherence and business requirements for risk responsiveness. Such conflict among agents leads to rationales for actions that are inconsistent, ad hoc solutions, which are hard to implement or hard to adapt in the future. Hence:

P1: Agents' perceived lack of fit negatively influences agents' perception of legal, technological and business risk

1.4.3 Control patterns reduce agents' perceived lack of fit

The second stream of research deals with the last two stages of the process put forward by Straub and Welke [230]: decision and implementation. Here one can refer to the work of Hoffman et al. [112] for compliance checking and to Bellamy et al. [18] for compliance visualization. The existence of a large set of IT solutions on the market for automatic control should also be acknowledged; for example, Rasmussen [200] put forward a rough classification.

The general idea of such research is that a system is created to automatically collect all users' actions and perform data mining for compliance verification, according to predefined business rules. To extend the existing literature, it is necessary to borrow concepts from the business model literature and propose three elements to map the goals of the three agents with inconsistent goals. In line with Osterwalder and Pigneur [175], value proposition is defined here as a way to describe which agents' problems are solved and why the offer is more valuable than similar services from competitors. In my opinion, the value proposition of a control pattern is one of the concerns of the legal agent, who is in charge of justifying how these actions fit into the firm's overall strategy. The key activities required to enforce the business rules can also be associated with staff, machines and proprietary knowledge required to deliver the value proposition. This part of the model is most likely to be useful to the agent in charge of the technical infrastructure. Finally, this extension of business rules allows an assessment of the cost of each control activity to be made; different value propositions can be associated with different agents according to their objectives, in order to assess their return on investment. If the return on investment is positive, the agent will conform to the regulations rather than simply comply. This mostly concerns the business agent, who is in charge of ensuring that the firm is profitable. In conclusion, it is seen as better to substitute the concept of a rule with the idea of a pattern, that is, to say, a solution for a recurring problem. The reason for this is that a rule is often an 'If-Then' statement, whereas a pattern is a reference point that can be adapted to different problems. The rest of this thesis refers to patterns as ideal types of a typology, defined as " complex constructs that can be used to represent holistic configurations of multiple unidimensional constructs " [70]. Thus, ideal types are composed of a set of dimensions (first-order constructs), which are the building blocks of traditional theoretical statements and are somehow related among them. In this case, the patterns have three dimensions: value proposition, key activities and key resources, and a return on investment. The relationships among these dimensions are defined by the Business Model Ontology suggested by Osterwalder and Pigneur [175]. Accordingly, it is possible to state that:

P2: A control pattern is composed of its value proposition, a set of key activities and resources, and a return on investment.

Previous studies of control theory [64] have claimed that a proper set of controls can increase trust among agents and can increase the quality of the process that is controlled. In addition, it has already been claimed that if the return on investment is positive, the agent will conform to the regulations rather than simply comply. By increasing trust among agents and by shifting from compliance to conformity, it is expected that the agents' fit will increase. In other words, in the long term, agents who use the control patterns will end up competing less and cooperating more. Hence:

P3: Over time, a control pattern reduces the agents' perceived lack of fit.

1.4.4 A control framework allows adaptations when regulations change

An interesting finding by Straub and Welke [230] was related to the importance of ensuring a feedback loop to constantly improve the compliance support system. Therefore, the last part of this model concerns the development of new patterns. A first consideration relates to who should be in charge of creating these patterns. To simplify the model, I have assumed the existence of a third party, who is in charge of aligning agents with inconsistent goals. Thanks to the decision already made to use concepts borrowed from the business model literature, it is much easier to describe the third party as a so-called infomediary [101]. Experience tells us that, in some situations, infomediaries are not present. In those cases, it is possible to verify the existence of the infomediary features spread out among agents, which become self-organized. A second consideration regards the creation and testing of new patterns. On the one hand, the creation of new ideal types should lead to the creation of new first-order constructs, which eventually will be organized in a hierarchy. On the other hand, according to Doty and Glick [70], a typology is tested by checking how far its ideal types differ from reality (i.e., profile similarity). It is proposed that the performance indicator for this typology be the agents' fit and that agents be in charge of proposing new items in the control framework. If agents are mostly competing, one could anticipate they will be motivated to write new items to influence the control framework and to shift the power balance toward themselves. In other words:

P4: If lack of fit among agents increases, then the number of items of the overall framework increases too.

Nevertheless, each control item reflects the perception of one agent, since it represents the reality to which that agent would like to conform. Hence, by combining different control items in the framework, it is possible to obtain a representation of agents' perceived reality;

a grounded theory, according to Glaser and Strauss [92]. This grounded theory can be compared to the existing control standards proposed by practitioners' organizations (e.g., ISO 27001, Isaca CobiT or OECG Red Book). Therefore, the use of pre-existing codes automatically provides the items of the control framework. It is then possible to assess the influences of different items by testing them in triplets using scenario-based surveys, a form of assessment successfully implemented in previous studies of information system security [15]. Such surveys will be given to regulated agents to estimate the effect of a combination of items on their intention to conform. One could expect that agents will conform to the items they have proposed; conversely, they will oppose items felt to be proposed by someone else. What is of particular interest here, however, are the reaction of agents to the combination of different items. This way, it is possible to assess whether two items deal with the same underlying idea or if one item can be removed because of scarce influence. The best-performing triplets (value proposition-key activities and resources-return on investment) are then converted into control patterns and enforced. It is reasonable to believe that at the beginning, most items will lead to control patterns, whereas after a while, few items will have significant effects compared to the existing ones. Thus:

P5: If the number of control items increases, then the number of control patterns increases.

1.5 Evaluation of the artifacts

In this section I clearly identify the link between research sub-questions, the artifacts developed, evaluation techniques used, and theoretical contributions, as expressed in figure 1.4 and presented in detail in the following section.

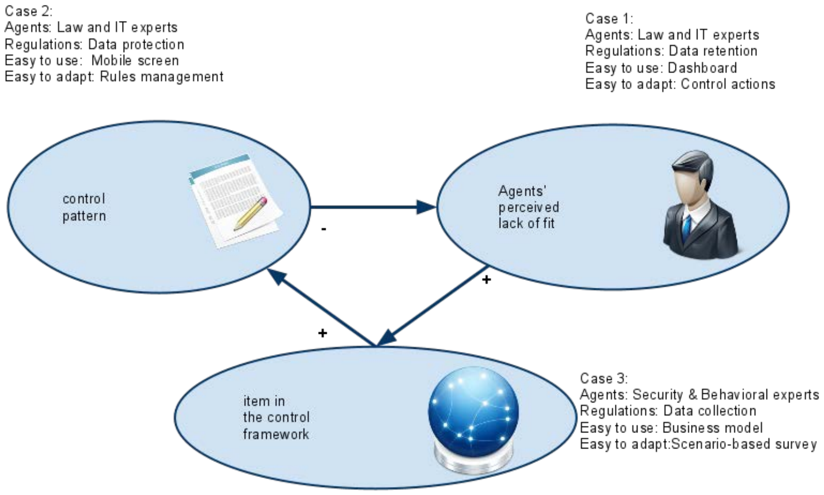

Case 2:
Agents: Law and IT experts
Regulations: Data protection
Easy to use: Mobile screen
Easy to adapt: Rules management
Case 1:
Agents: Law and IT experts
Regulations: Data retention
Easy to use: Dashboard
Easy to adapt: Control actions
control pattern
-
Agents' perceived lack of fit
+
+
item in the control framework
Case 3:
Agents: Security & Behavioral experts
Regulations: Data collection
Easy to use: Business model
Easy to adapt:Scenario-based survey

Figure 1.4: Artefacts evaluation

Phase 0: Understanding the problem and developing the main assumption. In the first phase, the central assumption of this thesis was not associated with an evaluation.

As part of this phase, however, I published an article that assesses the literature review in GRC and proposes a new approach to address the problem. This is presented in chapter 2 and represents my theoretical contribution.

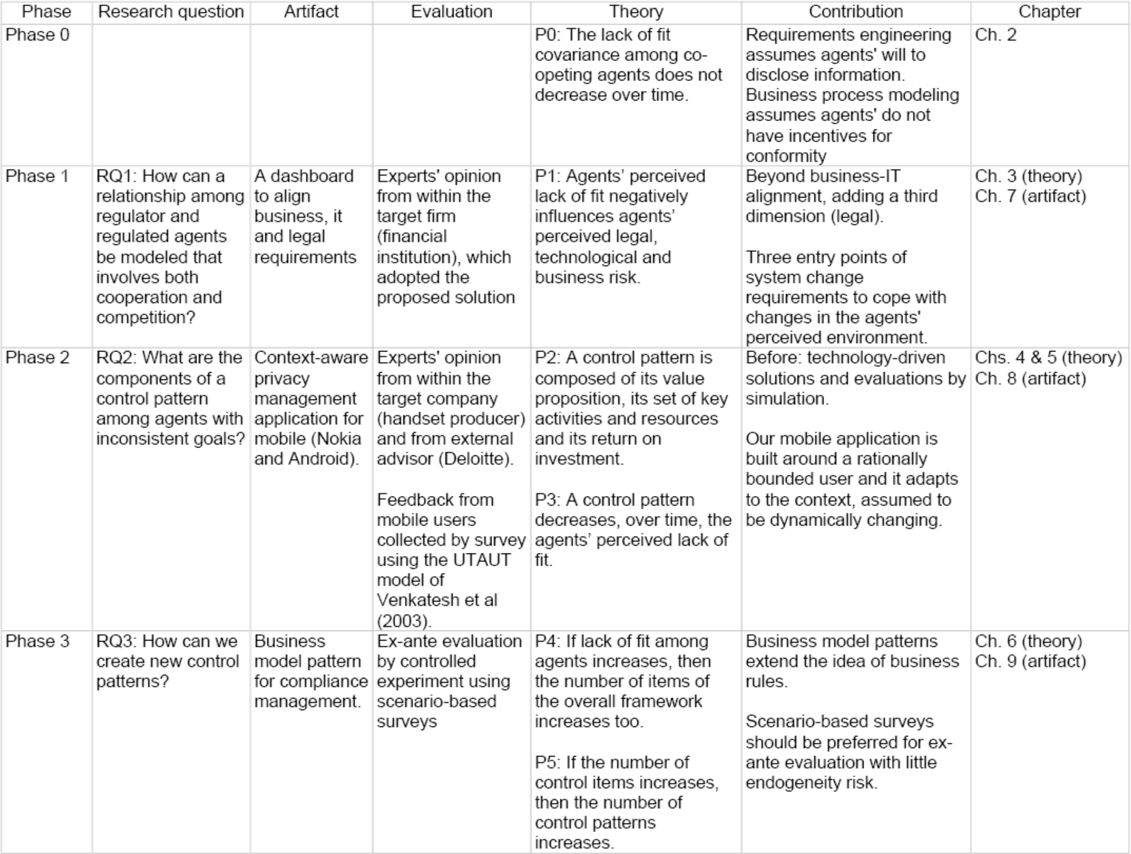
Phase 1: Developing a dashboard to align business, IT and legal requirements. The second phase addressed a situation of co-opetition among IT and legal agents with respect to regulations on data retention. A dashboard was developed to bring about easy-to-use alignment among agents' goals. A set of control actions was also defined to enable the system to easily adapt to new regulations. The dashboard was evaluated using experts' opinions from among the compliance officers in the financial institution in which the first case study was carried out. The dashboard design was adopted by the firm to model the compliance requirements at the corporate level; these were intended to be a positive outcome of the study. The outcomes of this phase are presented in chapter 3 (theoretical considerations around the dashboard) and chapter 7 (taxonomy of control actions for the dashboard).

Phase 2: Developing a context-aware privacy management application for mobile devices. The third phase addressed co-opetition among IT and legal agents with respect to regulations concerning data protection. A software application for mobile handsets was developed to bring about easy-to-use alignment among legal requirements about privacy and users' preferences. A set of rules was also defined to enable the system to easily adapt to new legal or user's requirements. Experts' opinions from within a handset company were collected and a usability test was performed with a small sample of mobile devices users from within the university. The UTAUT model of Venkatesh et al. [244] was used. Finally, I decided to collect external opinions, co-authoring a book chapter with an expert in privacy risk management from Deloitte SA. The outcomes of this phase are presented in chapter 8.

Phase 3: Designing a business model pattern for compliance management. The fourth phase addressed co-opetition among security and behavioural experts with respect to regulations on data collection. A business model pattern was developed to bring about easy-to-use representation of how to assure added value to all co-opeting agents. A way to conceive a scenario-based survey was also developed in order to assess possible variations of the business model pattern. The main goal was to assess the likelihood of success among mobile devices users for a set of strategies regarding privacy regulatory compliance: the reduction of collected data from users, the increase of data security controls (by means of the prototype developed in the previous iteration) and the exchange of non-monetary benefits for users' data (this would be the business dimension). Because this test implied causality, a control for endogeneity was introduced by combining the different control strategies and obtaining a set of scenario-based surveys. The surveys were given to a large sample of mobile devices users and the difference in response among respondent groups was assessed. Following an assessment of the different effects of the control actions, an overall framework was produced, which was represented using the business model ontology. The outcome of this phase is presented in chapter 9.

1.6 Form and structure

This section describes the overall structure of the thesis. It briefly underlines the findings presented in the chapters that follow; these findings are based on my articles published



Phase	Research question	Artifact	Evaluation	Theory	Contribution	Chapter
Phase 0				P0: The lack of fit covariance among co-opeting agents does not decrease over time.	Requirements engineering assumes agents' will to disclose information. Business process modeling assumes agents' do not have incentives for conformity	Ch. 2
Phase 1	RQ1: How can a relationship among regulator and regulated agents be modeled that involves both cooperation and competition?	A dashboard to align business, it and legal requirements	Experts' opinion from within the target firm (financial institution), which adopted the proposed solution	P1: Agents' perceived lack of fit negatively influences agents' perceived legal, technological and business risk.	Beyond business-IT alignment, adding a third dimension (legal). Three entry points of system change requirements to cope with changes in the agents' perceived environment.	Ch. 3 (theory) Ch. 7 (artifact)
Phase 2	RQ2: What are the components of a control pattern among agents with inconsistent goals?	Context-aware privacy management application for mobile (Nokia and Android).	Experts' opinion from within the target company (handset producer) and from external advisor (Deloitte). Feedback from mobile users collected by survey using the UTAUT model of Venkatesh et al (2003).	P2: A control pattern is composed of its value proposition, its set of key activities and resources and its return on investment. P3: A control pattern decreases, over time, the agents' perceived lack of fit.	Before: technology-driven solutions and evaluations by simulation. Our mobile application is built around a rationally bounded user and it adapts to the context, assumed to be dynamically changing.	Chs. 4 & 5 (theory) Ch. 8 (artifact)
Phase 3	RQ3: How can we create new control patterns?	Business model pattern for compliance management.	Ex-ante evaluation by controlled experiment using scenario-based surveys	P4: If lack of fit among agents increases, then the number of items of the overall framework increases too. P5: If the number of control items increases, then the number of control patterns increases.	Business model patterns extend the idea of business rules. Scenario-based surveys should be preferred for ex-ante evaluation with little endogeneity risk.	Ch. 6 (theory) Ch. 9 (artifact)

Figure 1.5: Artifacts Evaluation

in peer-reviewed conferences and journals. Figure 1.5 shows the link between research sub-questions, the artifacts developed, evaluation techniques used, theoretical contributions, and published articles presented in the following chapters of this thesis.

1.6.1 Structure of the thesis

This thesis is a collection of articles published between 2008 and 2011 in conference proceedings and journals belonging to the information systems and requirement engineering communities. The first chapter is intended to introduce the reader to the topic and to give a coherent and consistent view of the problem in hand, as well as the methodology and proposed solutions. The following chapters present the published articles in a coherent formatting style, although no changes in content have been made to the published versions.

1.6.2 Research publications

The following paragraphs outline my research publications, starting with their complete references. A brief summary of the article is given, followed by an assessment of the contribution each article makes to the overall framework. Such contributions are illustrated graphically using a subset of figure 1.5, presented in the previous section, to link research sub-questions, artifacts and publications. To conclude, some important findings of each article are highlighted.

1.6.3 Main assumption: Co-opeting agents

Reference for chapter 2: [27] Bonazzi, R., Hussami, L., & Pigneur, Y. (2008). Compliance management is becoming a major issue in IS design. Presented at the Conference of the Italian Chapter of the Association of Information Systems (ItAIS 2008), Paris: Springer.

Summary: Up to 2008, there was an absence of IT GRC models and standards that considered compliance management as an aligning function between governance and risk management. Such alignment implies an extension of the standard business-IT alignment proposed by Henderson and Vekatraman [107]. This led to the concept of ontological distance put forward by Rosemann et al. [208] as a way to measure agents' fit.

Contribution to the overall framework: This chapter introduces the agents to be aligned as described in the top part of figure 1.5.

Findings: My IT-Law alignment framework was used to assess the existing literature in IT GRC and to induce a null proposition (P0 in my theoretical framework), based on the evidence of conflicting goals among legal, technical and business agents. Accordingly, the IT GRC methodology used consisted of three cycles, shown in figure 1.6. The IT governance cycle identifies business opportunities and threats, steering the firm towards the minimization of business risk. The IT risk management cycle minimizing the impact of technological (e.g., security) threats over the goals of the company. The compliance management cycle is there to ensure that the directives coming from the governance management cycle are understood and executed by the risk management cycle, thereby minimizing the regulatory risk.

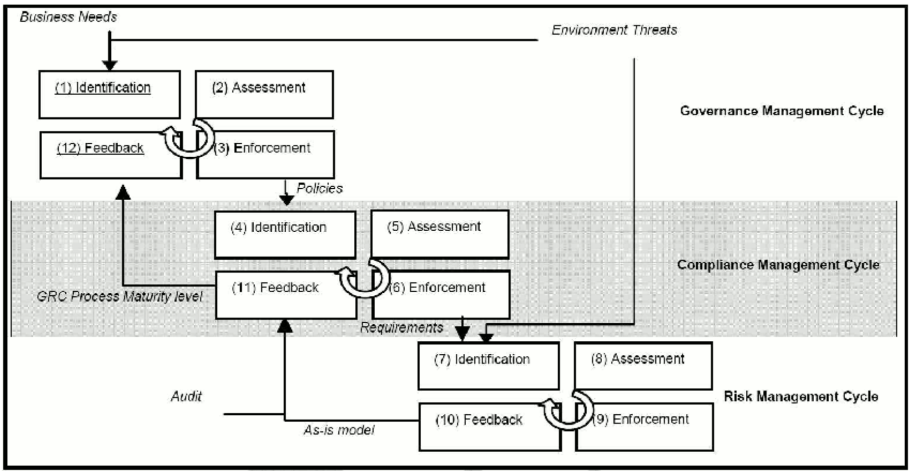


Figure 1.6: The IT GRC process

1.6.4 Problem analysis: Compliance among co-opeting agents

Reference for chapter 3: [29]Bonazzi, R., & Pigneur, Y. (2009). Compliance Management in Multi-actor Contexts. Proceedings of GRCIS 2009 workshop. Amsterdam.

Summary: This article aims to improve information systems management support to the Risk and Compliance Management process; that is to say, the management of all compliance imperatives that impact on an organization, including both legal and strategically self-imposed imperatives. We proposed a process to achieve such regulatory compliance by aligning the Governance and Risk Management activities. It was also suggested that Compliance should be considered as a requirement for the Risk Management platform.

Contribution to the overall framework: This chapter introduces a compliance dashboard that was designed and created for a private bank as an example of a compliance support system. Illustrated in the top part of figure 1.5 is the alignment of the co-opeting agents.

Findings: I propose a dashboard design to align law, business and IT compliance requirements. Figure 1.7 represents the result of our time spent with the IT compliance officer of the financial institution, whose data have been removed from the image to respect confidentiality. One can identify a list of boxes of different sizes. The big boxes are “libraries,” or a list of objects available. The user can draw a 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 whilst IT issues are hidden to the most users, allowing them to discuss the way to align IT services and law/business requirements. This supports proposition P1 in my theoretical framework by illustrating that fit among agents can be reduced by aligning the three dimensions presented in figure 1.7.

The top part of the figure. The business level of the company is represented, together with the collection of business entities, which are composed of business units. The small squares refer to the regulations, to which each business line and entity is subjected. If a business entity is subjected 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 yet comply, whilst the business unit in the USA gets an orange box around SOX if a project which has to comply with the law has been started but not yet finished.

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 IDs, expressed in circles. The color of the circle tells if the control activity is conceived to reduce the risk by requiring a preventive, proactive or reactive stance. In this manner, Sarbanes-Oxley might have “SOX” as its ID, and it might require “ensure internal control” as the control activity, which is a preventing/proactive activity. To define the control activities I referred to COSO and CobiT.

The bottom part of the figure. The IT solutions currently owned by the enterprise find their place here. Each IT solution is conceived to support at least one control activity. Thus, Enterprise GRC software, such as BWise, might support the “ensure internal control” activity.

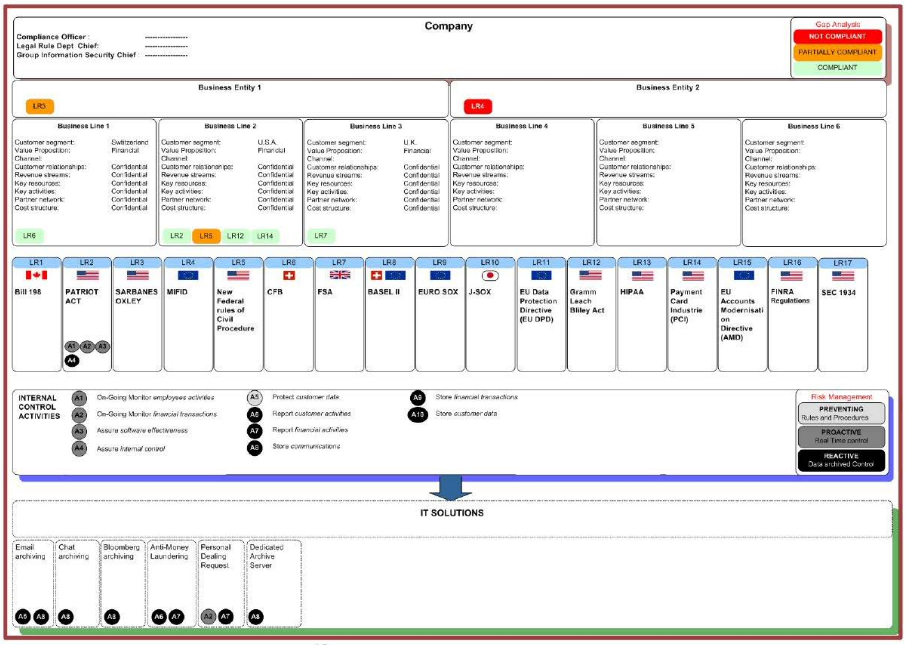

Company
Compliance Officer : ------------------
Legal Rule Dept Chief: ------------------
Group Information Security Chief : ------------------
Gap Analysis
NOT COMPLIANT
PARTIALLY COMPLIANT
COMPLIANT
Business Entity 1
LR3
Business Entity 2
LR4
Business Line 1
Customer segment: Switzerland
Value Proposition: Financial
Channel:
Customer relationships: Confidential
Revenue streams: Confidential
Key resources: Confidential
Key activities: Confidential
Partner network: Confidential
Cost structure: Confidential
LR6
Business Line 2
Customer segment: U.S.A.
Value Proposition: Financial
Channel:
Customer relationships: Confidential
Revenue streams: Confidential
Key resources: Confidential
Key activities: Confidential
Partner network: Confidential
Cost structure: Confidential
LR2
LR5
LR12
LR14
Business Line 3
Customer segment: U.K.
Value Proposition: Financial
Channel:
Customer relationships: Confidential
Revenue streams: Confidential
Key resources: Confidential
Key activities: Confidential
Partner network: Confidential
Cost structure: Confidential
LR7
Business Line 4
Customer segment:
Value Proposition:
Channel:
Customer relationships:
Revenue streams:
Key resources:
Key activities:
Partner network:
Cost structure:
Business Line 5
Customer segment:
Value Proposition:
Channel:
Customer relationships:
Revenue streams:
Key resources:
Key activities:
Partner network:
Cost structure:
Business Line 6
Customer segment:
Value Proposition:
Channel:
Customer relationships:
Revenue streams:
Key resources:
Key activities:
Partner network:
Cost structure:
LR1 Bill 198
LR2 PATRIOT ACT
A1 A2 A3 A4
LR3 SARBANES OXLEY
LR4 MIFID
LR5 New Federal rules of Civil Procedure
LR6 CFB
LR7 FSA
LR8 BASEL II
LR9 EURO SOX
LR10 J-SOX
LR11 EU Data Protection Directive (EU DPD)
LR12 Gramm Leach Bliley Act
LR13 HIPAA
LR14 Payment Card Industrie (PCI)
LR15 EU Accounts Modernisation Directive (AMD)
LR16 FINRA Regulations
LR17 SEC 1934
INTERNAL CONTROL ACTIVITIES
A1 On-Going Monitor employees activities
A2 On-Going Monitor financial transactions
A3 Assure software effectiveness
A4 Assure internal control
A5 Protect customer data
A6 Report customer activities
A7 Report financial activities
A8 Store communications
A9 Store financial transactions
A10 Store customer data
Risk Management
PREVENTING
Rules and Procedures
PROACTIVE
Real Time control
REACTIVE
Data archived Control
IT SOLUTIONS
Email archiving
A6 A8
Chat archiving
A8
Bloomberg archiving
A8
Anti-Money Laundering
A6 A7
Personal Dealing Request
A2 A7
Dedicated Archive Server
A8

Figure 1.7: Chapter 3: The design of the artifact's interface

1.6.5 Characteristics of the solution: The three components of control patterns for compliance

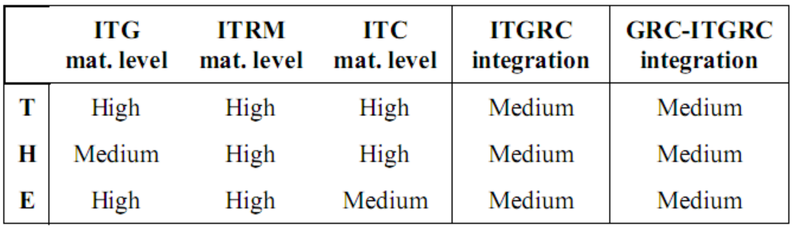
Reference for chapter 4: [192] Racz, N., Weippl, E., & Bonazzi, R. (2011). IT Governance, Risk & Compliance (GRC) Status Quo and Integration. Proceedings of the First International Workshop on IT Governance, Risk and Compliance (ITGRC 2011). Washington D.C.

Summary: The integration of GRC activities has gained importance over the last few years. This paper presents an analysis of GRC integration efforts in the information technology departments of three large enterprises. Action design research was used to organize the research in order to assess IT GRC activities based on a model with five dimensions. By means of semi-structured interviews, key findings were identified and rated concerning the status quo of the three IT GRC disciplines, their integration and their relation to GRC on the corporate level. Five key findings explained the main commonalities and differences observed.

Contribution to the overall framework: This chapter introduces the concept of control pattern described in figure 1.5 as a self-enforcing contract (implicit or explicit) among agents.

Findings: The interviews with the three companies showed evidence of control patterns implemented to align the three types of agent, thereby supporting P2 in my theoretical framework. Based on those interviews, we built a typology of IT GRC control patterns, shown in figure 1.8. The answers were analyzed and compared, and they were rated in five dimensions of a model derived from the literature review: the maturity level of the IT governance (ITG), the maturity level of the IT risk management (ITRM), the maturity level of the IT compliance process (ITC), the degree of integration among ITG, ITRM and ITC (ITGRC), and the degree of integration among corporate-level GRC (GRC-ITGRC).

The dimensions are first-order constructs used to describe all possible ideal types in theory [70]. All dimensions can have one of three possible values representing the maturity level of their processes, using the framework of the IT policy compliance group [98]: "high" for a score of 4 or higher out of 5, "low" for a score below 2 and "medium" otherwise. The values of ITGRC and GRC- ITGRC integration can never be greater than the average of the ITG, ITRM and ITC values. It is interesting to find that the three firms differ in their results according to their strategic intent, leading us to believe that control patterns are best suited to represent IT GRC among co-opeting agents (the integration of business unit is intended here).



	ITG mat. level	ITRM mat. level	ITC mat. level	ITGRC integration	GRC-ITGRC integration
T	High	High	High	Medium	Medium
H	Medium	High	High	Medium	Medium
E	High	High	Medium	Medium	Medium

Figure 1.8: IT GRC ideal types

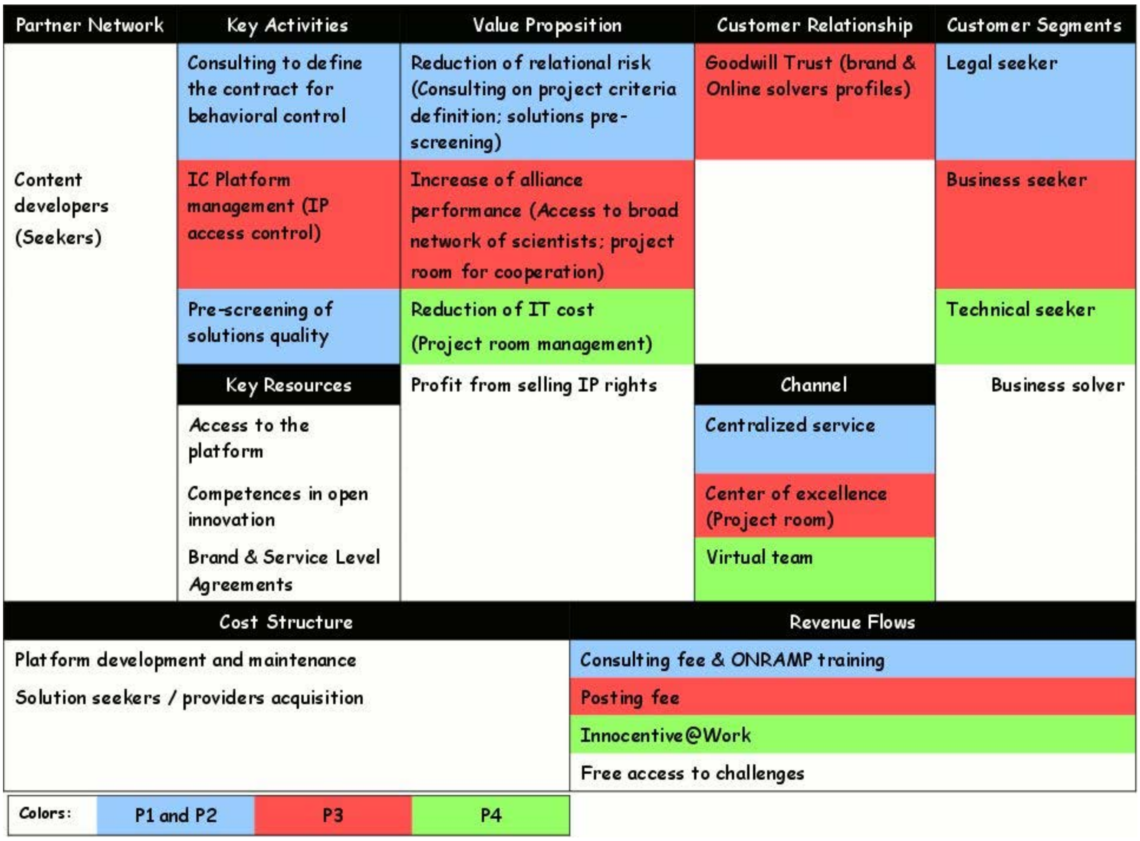
1.6.6 Solution design: A third-party for compliance support

Reference for chapter 5: [26]Bonazzi, R., Golnam, A., Pigneur, Y.,& Wegmann, A. (2012). Respecting the deal: Economically sustainable management of open innovation among co-opeting companies. International Journal of E-Services and Mobile Applications. Forthcoming

Summary: Platforms such as eBay allow product seekers and providers to meet and exchange goods. On eBay, consumers can return a product if it does not correspond to expectations; eBay is the third-party firm in charge of ensuring that the agreement between seekers and providers will be respected. This raises the question of who provides the same service for open innovation, where specifications might not be fully defined. This paper describes the business model of an organizational structure that supports the elicitation and respect of agreements among agents with conflicting interests, but who gain by cooperating. Building on previous studies, our business model takes into account the economic dimensions that relate to the needs for knowledge sharing and mutual control; these allow a third party to sustainably reinforce trust among untrusted partners and to lower their overall relational risk.

Contribution to the overall framework: This chapter deals with contract sustainability among co-opeting agents who have to comply with it, as illustrated in figure 1.5.

Findings: The existing literature in system dynamics was combined with that relating to the resources-based view, transaction costs and game theories. We used the business model ontology introduced by Osterwalder et al. [176] to obtain the business model components of a third-party agent illustrated in figure 1.9. The analysis of existing literature supports our claim that such trusted third-party agents can align the co-opeting agents' goal into a self-enforcing contract that reduces the agents' perceived ontological distance (P3 of my theoretical framework). Existing research has already proposed different control strategies for infomediaries, and we cite here the most recent work presented by Koch and Shultze [132]. In our opinion, we build on such models by underlying the alignment of the third-party value proposition and co-opeting agents' goals, the required level of trust that the third party has to acquire by having certifications, and the key resources that the third party needs to possess to enable the control strategies to have an overview of the expected profit and cost of the third party.



Partner Network

Content developers (Seekers)

Key Activities

🟦 Consulting to define the contract for behavioral control

🟥 IC Platform management (IP access control)

🟦 Pre-screening of solutions quality

Key Resources

Access to the platform

Competences in open innovation

Brand & Service Level Agreements

Value Proposition

🟦 Reduction of relational risk (Consulting on project criteria definition; solutions pre-screening)

🟥 Increase of alliance performance (Access to broad network of scientists; project room for cooperation)

🟩 Reduction of IT cost (Project room management)

Profit from selling IP rights

Customer Relationship

🟥 Goodwill Trust (brand & Online solvers profiles)

Channel

🟦 Centralized service

🟥 Center of excellence (Project room)

🟩 Virtual team

Customer Segments

🟦 Legal seeker

🟥 Business seeker

🟩 Technical seeker

Business solver

Cost Structure

Platform development and maintenance

Solution seekers / providers acquisition

Revenue Flows

🟦 Consulting fee & ONRAMP training

🟥 Posting fee

🟩 Innocentive@Work

Free access to challenges

Colors: 🟦 P1 and P2 🟥 P3 🟩 P4

Figure 1.9: Third-party business model

1.6.7 Artifact mutability: Creation of new control patterns

Reference for chapter 6: [24]Bonazzi, R., Checcaroli, C., & Missonier, S. (2011). The man behind the curtain. Exploring the role of IS strategic consultant. 6th International Workshop on BUSiness/IT ALignment and Interoperability (BUSITAL 2011). London, UK.

Summary: Most organizations encounter business-IT alignment problems because they fail to properly understand how well an enterprise software package aligns with or fits their needs. Strategic consultants make a profit by reducing such external manifestations of the differences between the organization's needs and the system's capabilities. Therefore, it appears relevant to understand how consultants behave.

Contribution to the overall framework: This chapter focuses on the control framework, which is shown in figure 1.5 and is used by strategic consultants to create control patterns used with their clients.

Finding: Our theoretical model showed how a consultancy can assess the way to extract and to generalize knowledge from its clients, supporting P4 and P5 of my theoretical framework. The loss derived from sharing the consulting firm's global knowledge is balanced with new local knowledge obtained from the client. Thus, it was possible to assess the quality of that contribution and the mutual knowledge exchange.

1.6.8 A compliance management dashboard for a private bank

Reference for chapter 7: Bonazzi, R. & Pigneur, Y. (2011). A set of control actions for a compliance support system used in a financial institution. Working paper.

Summary: In this paper, we address the elicitation of information system requirements for regulatory compliance, intended as a group decision between actors with conflicting goals. Building on the solutions proposed by previous authors in the field of multi-actor requirement engineering for multi-regulation compliance, we claimed that a set of patterns describing compliance-oriented services will lead to efficient, consistent and sustainable requirements for the information system. We illustrated the current state of the development of a typology, which were presented at the conceptual level, by means of its constructs, principles of form and functions. A fictive scenario inspired by a real case allowed us to discuss the flexibility required to adapt the requirements to the evolution of regulations. We concluded with some testable propositions to falsify our typology, together with highlights of the directions we intend to follow in order to obtain a handbook of patterns for regulatory compliance.

Contribution to the overall framework: As shown in figure 1.5, this chapter presents the first application of the theoretical framework. It is derived from our first practical experience regarding regulatory compliance.

Findings: We coded the set of requirements using the common standards for Enterprise Risk Management and compliance (that is COSO ERM and CobiT). In this way, we were able to produce a paper version of a dashboard to map a limited number of legal, business and technical requirements. To evaluate the model, we used opinions from experts in the company. These experts adopted the dashboard as an approach to further model legal, business and technical requirements. More detailed problem analyses were performed and we extended our scope to include economically viable compliance systems among co-opeting companies, such as IT outsourcing and open innovation. Hence, we performed action research by taking part in a three-month project with a second financial institution. We collected functional and non functional requirements for contract management when outsourcing data management tasks. We coded these requirements using the business model ontology [175] 9 building blocks.

1.6.9 A privacy management application for mobile devices users

Reference for chapter 8: [28]Bonazzi, R., Liu, Z., Garniere, S., & Pigneur, Y. (2011). A dynamic privacy manager for compliance in pervasive computing. IGI Global.

Summary: In this paper, we propose a decision support system for privacy management in context-aware technologies. Such a system requires the alignment of four dimensions: business, regulation, technology and user behavior. We aimed to develop a mid-range theory in the form of a typology of control actions. By following a telecommunication training course for application programmers, we developed a prototype for privacy management to instantiate a set of control actions for privacy. The control actions were ideal types, which had two values: one regarding the risk addressed and the way to detect it, and one regarding the technology used. To code these risks, we used the OECD guidelines for data privacy [78].

Contribution to the overall framework: As shown in figure 1.5, this chapter presents the application of the framework to develop privacy management software for mobile devices users.

Findings: We developed a middleware model able to achieve compliance with privacy policies within a dynamic and context-aware risk management situation. We were able to illustrate our model in more detail by the development of a small prototype,The current outcomes of its implementation were presented, enabling us to identify the possible direction of future investigation.

1.6.10 Compliance support business model patterns for privacy

Reference for chapter 9: [145]Liu, Z., Bonazzi, R., Fritscher, B., & Pigneur, Y. (2011). Privacy-friendly Business Models for Location-Based Mobile Services. Journal of Theoretical and Applied Electronic Commerce Research, 6(2).

Summary: The elicitation of regulatory requirements and compliance certification are the bottlenecks of the current compliance management cycle. Therefore, we tested a solution that allows the ideal types to be extracted from a crowd by a third party; the crowd can also be used to test the ideal type's likelihood of usage. In our test, we fixed the regulatory certification to a privacy regulation in the U.K. Three different approaches were checked: reduction of collected data, increase of data protection, and increase of distributive justice (to exchange the user data with some non-monetary benefit). In our case, the co-opeting agents were the mobile user who sends data and the mobile provider who collects that data.

Contribution to the overall framework: As shown in figure 1.5, this chapter applies the methodology suggested by our framework to obtain a set of control patterns, which are then converted into theory-driven business models.

Findings: It was shown that different groups of mobile device users give different scores to these approaches. We derived a business model for a third party in charge of obfuscating the identity of some mobile device users and of ensuring proper compensation for users who are less concerned about privacy. Its business model is presented in figure 1.10. Our findings led us to claim that a self-enforcing control pattern can be obtained by collecting agents' goals and by assessing agents' perceived ontological distance. This builds on the work of information systems researchers grounded in psychology, such as Cavusoglu et al. [38], since our intent is to use quantitative results to derive business model prescriptions.

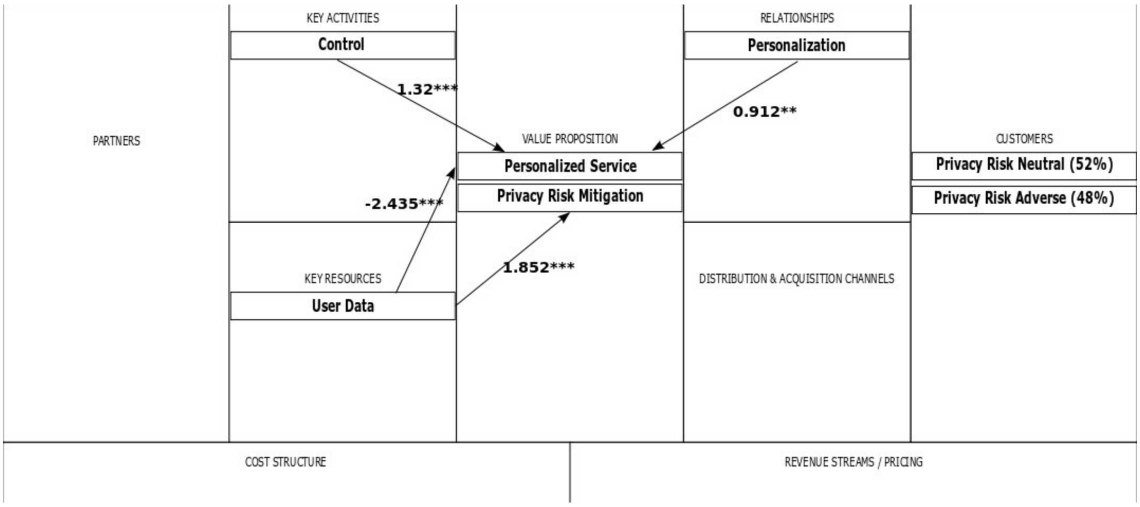


Figure 1.10: Compliance theory-driven business model for trusted third-party

1.6.11 Extension number 1: A compliance support system for education

Reference for chapter 10: [24]Bonazzi, R., Missonier, S., Jaccard, D., Bienz, P., Fritscher, B., & Fernandes, E. (2011). Analysis of serious games implementation for project management courses. Proceeding of the 8th Conference of the Italian Chapter of AIS (ItAIS 2011). Rome.

Summary: One of the major criticism addressed at our model concerns the lack of possible applications in employees' compliance training. Therefore, we decided to describe how a compliance support system could include simulation in order to assess hypothetical cases and train students. The opportunity to test our idea was presented during a project in which project management students had to use the system to know how to comply with a teacher's expectations in order to pass the final exam. Previous research into pedagogy and project management have already underlined the positive contribution of serious games to project management courses; however, the empirical outcomes of these studies have not yet been translated into functional and technical specifications for the designers of such games. Our study aims to obtain a set of technical and functional design guidelines for serious game scenario editors, to be used in large classes of project management students.

Contribution to the overall framework: This chapter adds the idea of control patterns and intrinsic motivation to agents' training in the context of compliance.

Findings: We conceived a framework to assess the influence of different serious games components over students' perceived acquired competency. Such frameworks will allow us to develop a software module for reflective learning, which is meant to extend the theory of serious games design. The results that we have obtained thus far lead us to believe that serious game design has both a direct and an indirect effect over students' perceived acquired competency, which is mediated by students' engagement. The results that we have obtained show that serious game design also has a direct effect over students' acquired competencies that is statistically significant. It also appears that the students' engagement has an effect on the students' perceived acquired competency that is statistically significant. Finally, serious game design has an effect on the students' engagement that is statistically significant. The module we wish to develop in the future has a graphical interface that allows the scenario designer to represent the scenario as a graph. The module is expected to be able to mine the log of student groups' actions and to represent them in the form of graphs in order to benchmark the different groups' experiences.

1.6.12 Extension number 2: An adaptive compliance support system

Reference for chapter 11: [25] Bonazzi, R., Fritscher, B., Liu, Z., & Pigneur, Y. (2011). From "Security for Privacy" to "Privacy for Security." Proceedings of the Second International Workshop on Business Models for Mobile Platforms. Berlin.

Summary: Our proposed compliance support system framework elicited a remark that addresses the costs associated with the degree of automation of its rule generation process. Although we believe that in most cases a large part of the rule generation task should be performed by humans (experts and users), sometimes the user is also the expert. Hence, it might be possible to automatically generate rules according to users' behaviours. This article envisions the use of context-awareness to improve single sign-on solutions (SSO) for mobile device users. The attribute-based SSO is expected to increase users' perceived ease of use of the system and service providers' authentication security of the application. From these two features, we derived two value propositions for a new business model for mobile platforms. The business model can be considered as an instantiation of the privacy-friendly business model pattern presented in our previous work, reinforcing our claim that privacy-friendly value propositions are possible and can be used to obtain a competitive advantage.

Contribution to the overall framework: This chapter adds the idea of automation of control patterns generation and testing.

Findings: From a cognitive point of view, usability issues arise when users cannot properly manage the information required to sign in to different web services using a large set of different pseudonyms and passwords. The possibility of capturing the change in the identity of the real user (the features of his or her everyday life behavior) has been considered only as a threat to his or her privacy. We propose to shift from a discretionary access control approach to an attribute-based approach, where the attributes are features of the user's environment and his or her behavior in that context. We see great potential in this possible threat. Thus, we formulated our starting assumption in the form of a null proposition for this adaptive compliance support system: namely, that context is a unique user identifier. We defined authentication security as the number of true positives and true negatives obtained by the system. In other words, we aim to minimize the number of occurrences in which the user is not allowed to access the system (false negative) or an unauthorized person is allowed to access the system (false positive). Hence, we hope that the first three propositions will have a stronger effect than the fourth one: the conjoint effect of time and location increases authentication security; the conjoint effect of time, location, and activity increases authentication security; the conjoint effect of time, location, activity and identity increases authentication security; and the conjoint effect of time, location, activity and identity increases ease of use. The theoretical model is currently being tested using a specific Nokia users' database with a large set of longitudinal data.

1.7 Contributions

In this section I start by addressing the three research sub-questions and then convert my results into a set of actionable guidelines for practitioners. Figure 1.11 presents a simplified version of the theoretical model, which I derived from the evidence collected while iteratively developing and testing my three artifacts. Such a framework should be considered as my overall contribution delivered at the end of my research, and hopefully as a starting point for a hypothetico-deductive study in the future.

1.7.1 Theoretical contributions

The following paragraph grounds the answers to the three research sub-questions in the proposed propositions and published papers. Each answer refers to guidelines produced by Davis [66] to define why its outcomes are theoretically interesting.

Research sub-question 1: How can a relationship between the regulator and regulated agents be modeled in order to involve both cooperation and competition? To answer this research sub-question, it is necessary to combine proposition 0 and proposition 1. Assuming that the covariance of the lack of fit among agents does not decrease over time (P0), agents' perceived lack of fit negatively influences agents' perceived legal, technological and business risk (P1).

That's interesting! What seems to be an individual phenomenon is in reality a holistic phenomenon [66]. Building on the idea of holistic compliance suggested by Volonino et al. [245], I proposed a Business-IT-Law alignment framework in chapters 2 and 3 that is similar to the idea of situational method engineering proposed by Gericke et al. [88]. In so doing so, this is believed to be the first attempt to propose that agents should model their perceived reality; scholars have assumed instead that it was up to them to develop a goals/process model. The collection of experts' opinions from within the target firm (a financial institution) supported my claims.

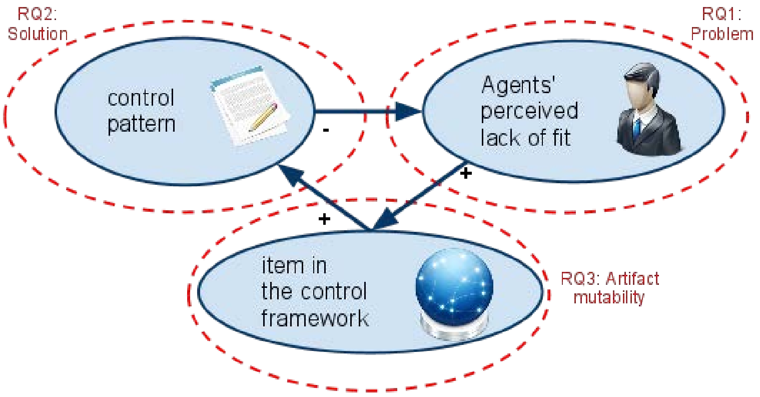


Figure 1.11: The concepts of my theoretical framework

Research sub-question 2: What are the components of a control pattern among agents with inconsistent goals?

This research sub-question can be answered by combining proposition 2 and proposition 3. A control pattern is a latent variable derived from its value proposition, from its set of key activities and resources, and from its return on investment (P2); such a control pattern reduces the agents' perceived fit (P3) over time.

That's interesting! What seems to be a phenomenon that function effectively as a means for the attainment of an end is in reality a phenomenon that functions ineffectively [66]. The type of control that focuses on process output quality could have a negative effect. It might increase compliance risk because it can lower agents' perceived trust, which negatively impacts their intrinsic motivation to respect the regulation. Instead of focusing on controls, I focused on agents' perceived pay-offs, proving that controls are effective if combined with solutions that increase agents' intrinsic motivation to comply. This claim was grounded in previous studies of control theory [64] To falsify such a claim regarding the importance of intrinsic motivation, chapter 8 presents small context-aware privacy management software for mobile devices that allows users to swing between data control for privacy and data sharing for context risk analysis. I speculated that such a type of application could lead to a set of profitable business models for a third party in charge of aligning agents with inconsistent goals. The collection of experts' opinions from within the target firm (a handset producer) and from outside the target firm (a consulting firm) supported my claims.

That said, it is worth noting recent work carried out by Koch et al.[132], which has been published on MISQ and supports my theory, even though I was not aware of it when developing my model. Their work focuses on intermediaries in electronic markets and identifies three main roles, which are similar to the three loops described in my model. Koch et al. also defined a set of useful implementation strategies, which are included in my model as critical activities. Therefore, I believe that my business model of a third party, and its nine building blocks, builds on previous literature by offering a deeper analysis of the required components.

Research sub-question 3: How can one create new control patterns that are easy to use and to adapt? This research sub-question can be answered by combining proposition 4 and proposition 5. If lack of fit among agents increases, then the number of items in the overall framework increases too (P4). Likewise, if the number of control items increases, then the number of control patterns also increases. (P5).

That's interesting! What seems to be stable and unchanging is in reality an unstable and changing phenomenon [66]. Although previous studies have already taken into account that regulations are constantly evolving, they have not questioned whether the equilibrium among regulated agents is constantly changing. Change can lead to the creation of a new regulation; change can also be due to a new technology that reduces the cost of controls or, for example, adds a new business opportunity. I took into account into account Gregor and Jones' idea of artifact mutability [96] and in chapter 2 I propose a workflow with different entry points that can initiate change. The system presented in chapters 5 and 9 describes a solution to automate the creation and testing of new patterns to adapt to change in the environment. To evaluate my system I collected opinions from strategic consultants and I performed statistical analysis using scenario-based surveys.

1.7.2 Answering the research question

By answering the three research sub-questions, it is possible to address the research question.

How to design easy-to-use and easy-to-adapt information systems for data retention regulatory compliance among co-opeting agents subjected to a large number of constantly evolving regulations?

The solution that I propose is a compliance support system. This approach focuses on agents' fit and it builds on previous research based on requirement engineering and business process management. This system was based on the theoretical model derived from the different studies conducted during the course of this study. It was also evaluated. The final result was the control scenario for the new theory-based business model. The compliance support system can be considered a design theory that, according to Gregor and Jones [96] should have:

- A purpose and a scope: the purpose of a compliance support system is cost reduction for data management regulatory compliance.
- Principles of form and function: three constructs (agents' fit, control pattern and control framework) are used to describe a compliance support system.
- Artifact mutability: the control framework is meant to extend the compliance support system with new control patterns to adapt to changes in regulation.
- Testable propositions: five propositions are defined among the three constructs used to describe a compliance support system.
- Justificatory knowledge: my compliance support system is based on control theory, contract theory and knowledge-based theory.
- Principles of implementation: descriptions of key components of the compliance support system and examples of its application are are given in the published articles.
- Expository instantiation: three artefacts were developed and evaluated to test my model: a dashboard, a mobile application and a business model pattern.

1.7.3 Contributions for practitioners

Because there is always tension between practitioners with regard to relevance and theoretical rigor, I have included a set of suggestions for IT GRC experts, derived from my study:

Stop hesitating between "control everything" and "trust everyone" strategies. Carefully choose the control level that your firm needs: my IT methodology presented in chapters 2 and 3 shows how agents' perceived lack of fit can be split into agents' perceived regulatory, technological and business risk.

Consider the possibility of adding a trusted third-party to decrease compliance management cost. The third-party business model presented in chapter 5 shows that a self-enforcing contract by a trusted third party reduces the agents' perceived fit over time.

Do not focus only on control. A self-enforcing contract composed of control patterns can align the agents' legal, technological and business goals. Refer to chapters 4 and 7 for examples of control patterns.

Reduce the cost of compliance management by partially automating the creation and test of control items for your ideal types. The test carried out in chapter 9 on control ideal types shows that self-enforcing contract goals can be elicited by agents' perceived fit.

1.8 Conclusions

The first chapter concludes with a short summary and a description of the limitations of this study.

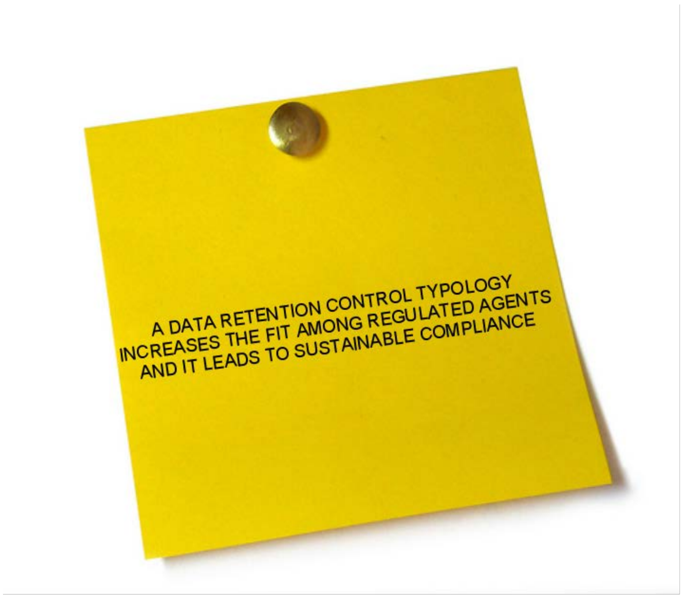

A DATA RETENTION CONTROL TYPOLOGY
INCREASES THE FIT AMONG REGULATED AGENTS
AND IT LEADS TO SUSTAINABLE COMPLIANCE

Figure 1.12: Conclusions

1.8.1 Summary

An academic once noted that at the end of your thesis you should be able to write its core idea on one Post-it note. Thus, figure 1.12 is my attempt to summarize the issues raised so far, in a few lines. By way of further elaboration:

- "A data retention control typology" deals with the second research sub-question and describes my proposed solution for using the concept of typology, intended as a collection of ideal types. Such ideal types can be considered as patterns, that is to say, solutions for recurring problems. They have three first-order constructs, which correspond to three agents with inconsistent goals (legal, business and technological). By referring to data retention control, the scope of the theory is limited by the data collected in my tests, even if further applications for this model do exist.
- "increases the fit among regulated agents"deals with the problem described at the beginning of this chapter, and which is addressed by the first research sub-question. The lack of fit among agents is my central assumption, whereas regulatory compliance is the current burden of multinational firms that have to comply with a large number of regulations. Based on the evidence collected in this study, it is claimed that this typology lowers this burden.
- "and it leads to sustainable compliance" deals with the idea of artifact mutability addressed by the third research sub-question. Regulations are known to have constantly evolved in the last few years in response to crisis and disasters. Accordingly, companies must adapt their internal controls dynamically without letting their compliance management costs explode. Here, I proposed an original way to create and test new control patterns, and theorize on the evolution of patterns creation over time.

1.8.2 Limitations and further works

When discussing this work with colleagues, three remarks kept recurring; these remarks are acknowledged here. The first one addresses the decision to add a third party into the model to coordinate agents with inconsistent goals. Third parties are know to add costs and their presence might raise power concerns. The second remark concerns the generalization of this work. The proposed model has been tested in only a few companies; thus, it is very likely that it will behave differently in new contexts. Moreover, only the data retention concerns of IS regulatory compliance have been treated, with other important issues (e.g., employees training) not being considered. The third remark concerns the coherence of this work. Because I have been working with different companies and addressing different software components, it is very likely they will not always fit well together.

I am currently working to address the first two remarks by adding more tests and by removing the assumption of a third party. The two extensions, which have already been published, should give a hint about future work directions:

- Using a compliance support system in education: in some courses, students compete with each other to get the best grade but they have to work in groups to deliver a project at the end of the semester. The teacher is a regulator who cannot assess the complete knowledge of the student by means of the final test. Thus, I developed a system that collects the complete set of required skills the student should have at the end of the course and merges them into a simulation. It is hoped that the use of game-inspired mechanisms will increase the intrinsic motivation of students to conform to teachers' regulation, resulting in greater student commitment and higher grades at the end of the course. If that is the case, it is planed to start testing the tool to train company employees to comply to enterprise policies.

– Designing a dynamic compliance support system: in some cases the regulator and the regulated are the same person. When users access their mobile devices, they have to prove their identity by complying with a set of policies they have previously defined. It is difficult to define such policies because they are either too hard to use or too easy to break. By proposing a system that dynamically generates policies and automatically enforces them, it is hoped that a greater degree of protection and ease of use may be achieved.

It should be stated here that neither my aim - or current expectation - was to obtain something other than a mid-level theory; that is to say, a set of patterns that are expected to perform well for recurring problems in similar contexts. To move forward, the use of a more general theory may detract from the practical relevance of the proposed model. On the other hand, increasing the complexity of the model too much, in an attempt to include all the exceptions encountered, could lead to the model becoming less easy to use.

Part II

Part 2: Our research publications

Chapter 2

Compliance management is becoming a major issue in IS design

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.

2.1 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. IT Policy Compliance Group [98] 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. 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 Purdy [190], 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. Volonino et al. [245], Rasmussen [199], Gasser and Hausermann [87]). 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 2.1 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. More in details, the first three steps shown in figure 2.1 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 Kark et al. [130]. 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 McClean and Rasmussen [157]. 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 [130]. 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.

2.2 IT Compliance framework

For our IT GRC process model we combined the concept of a risk management cycle [235] and the ones of quality management IT Policy Compliance Group [98] together with the previous works of Giblin et al. [91] of IBM, Sheth [219] from Semagix and El Kharbili et al. [74], who proposed a compliance process life-cycle and described the process steps. Giblin [91] 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.

We propose the regulation/IT alignment framework illustrated in figure 2.2. This is aimed to recall the strategic alignment model of Henderson & Venkatraman [107] and it has four domains, as the product between dimensions and sources of regulations. For the sake of clarity, figure 2.2 presents a real example taken from practice, concerning requirement engineering for document retention compliance with SEC 17a-4. Comparing figure 2.2 with figure 2.1, one can notice that the Governance steps of the IT GRC process generate the

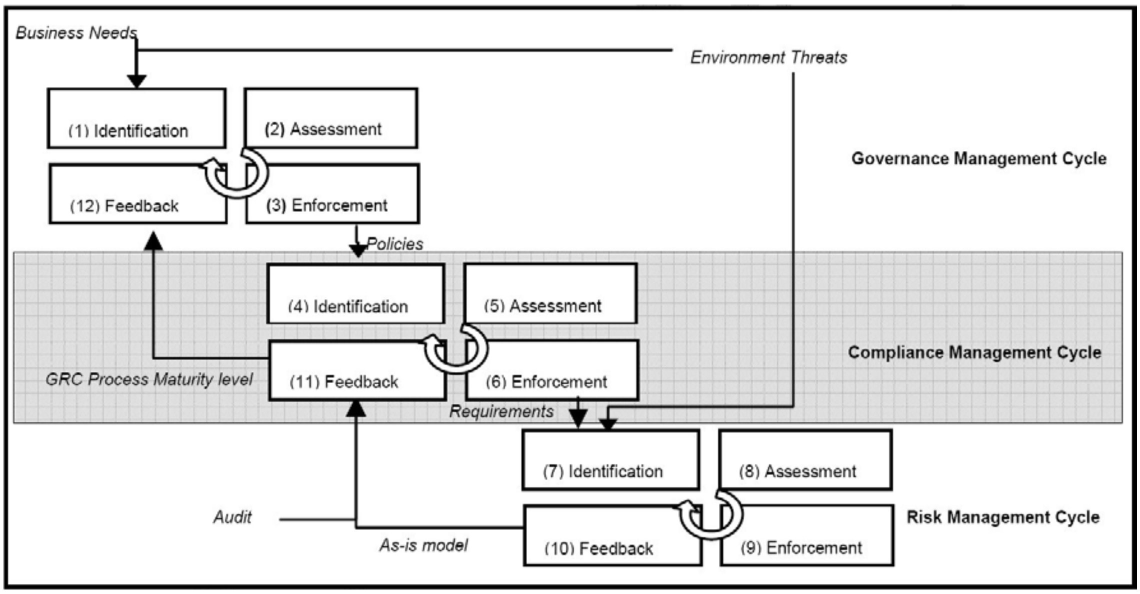
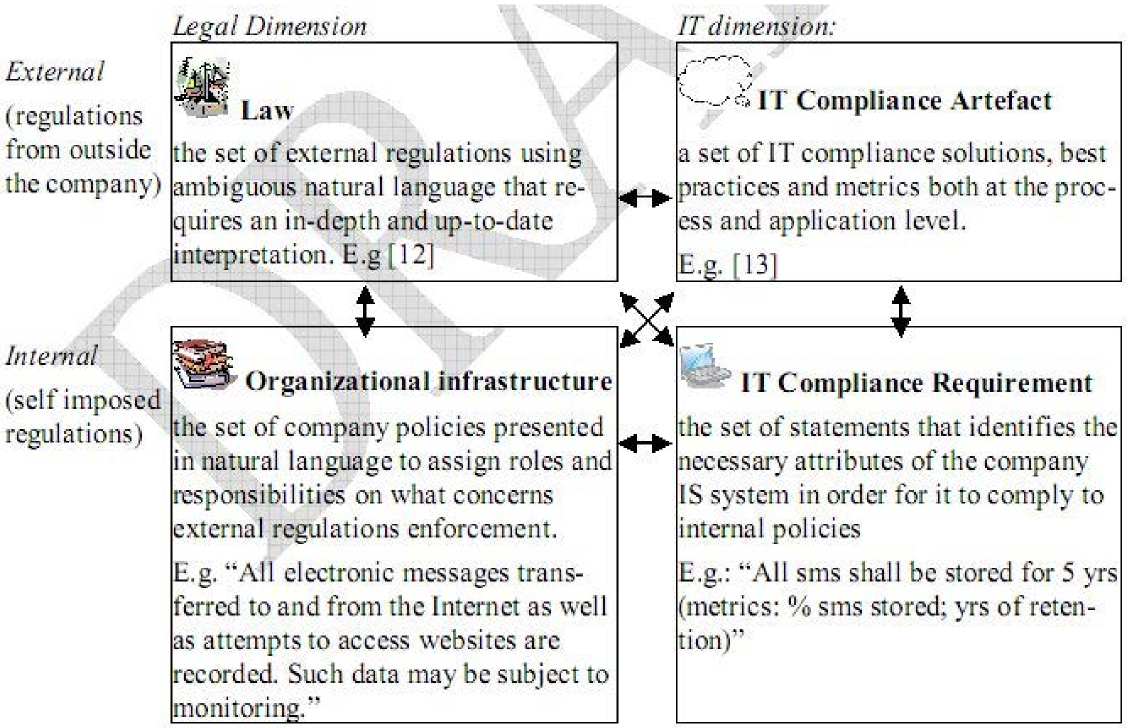


Figure 2.1: The IT GRC process

policies in the Organizational Infrastructure, while the Compliance steps deliver the IT Compliance Risk Management infrastructure.

2.3 Different alignments among domains

This section describes the different alignments in the framework presented in figure 2.2, 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 [56] for what concerns enforcement strategies. A support tool for the identification and assessment parts is proposed by Lau et al. [141], 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 [147]. 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 [122] 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



Legal Dimension

IT dimension:

External

(regulations from outside the company)

Law

the set of external regulations using ambiguous natural language that requires an in-depth and up-to-date interpretation. E.g [12]

IT Compliance Artefact

a set of IT compliance solutions, best practices and metrics both at the process and application level.

E.g. [13]

Internal

(self imposed regulations)

Organizational infrastructure

the set of company policies presented in natural language to assign roles and responsibilities on what concerns external regulations enforcement.

E.g. "All electronic messages transferred to and from the Internet as well as attempts to access websites are recorded. Such data may be subject to monitoring."

IT Compliance Requirement

the set of statements that identifies the necessary attributes of the company IS system in order for it to comply to internal policies

E.g.: "All sms shall be stored for 5 yrs (metrics: % sms stored; yrs of retention)"

Figure 2.2: Regulation / IT alignment

and Faltus[207] 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. [95] 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.[143] 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 and Stojanovic [164] 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. [3] from IBM, who proposed to see the internal controla 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 and Rosemann [261] 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” [206, 95, 143, 164, 3] 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. [106] offered a list of the most important in compliance process, Sheth [219] 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 [199], to a set of best practices [131] 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 [91, 219, 74]. Gangemi et al. [86] built a Core Legal Ontology (CLO) above an extension of their previous work DOLCE. Another considerable effort has been made by Hoekstra et al. [111] 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 [87] or Skinner’s idea of forensically evolving regulations [224]). We decided to call this alignment Awareness. The diagonal alignments. Even if many authors [98, 245, 131, 91, 219, 74] 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. [109] 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.

2.4 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 [245, 199]; 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 [164, 3, 261] at the business process level form a package and need to be integrated together. A coupling with a risk assessment tool [164] 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 involves 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 [85]) 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.

Chapter 3

Compliance Management in Multi-actor Contexts

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.

3.1 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 [157]). Should these policies and standards not be observed, "compliance risk" arises as, described by the main global regulator, the Basel Committee on Banking Supervision [174]. 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 [236] although some studies [98] 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 [156] 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. [16]. 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: (1) What artifact would support the multi-actor and constantly evolving process of IS compliance management facing ambiguity, traceability and efficiency? (2) 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.

3.2 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. [27], 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. [177] as they refer to compliance only as a control function. For what concerns compliance risk identification (step number 4 in figure 3.1) 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 [11] viewpoints integration game, through which the inconsistencies of non-canonical requirement specifications are resolved. The assessment step (step number 5 in figure 3.1) should follow the idea of holistic compliance proposed by [245]. 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 [52] and to perform gap analysis between compliance needs and existing solution in place [207], 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 [33] ontology-based extension of the Frame-Based Requirements Analysis Method. In this case Cheng et al [48] proposed a hierarchy between control activity objects. On what concerns enforcement (step number 5 in figure 3.1) 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

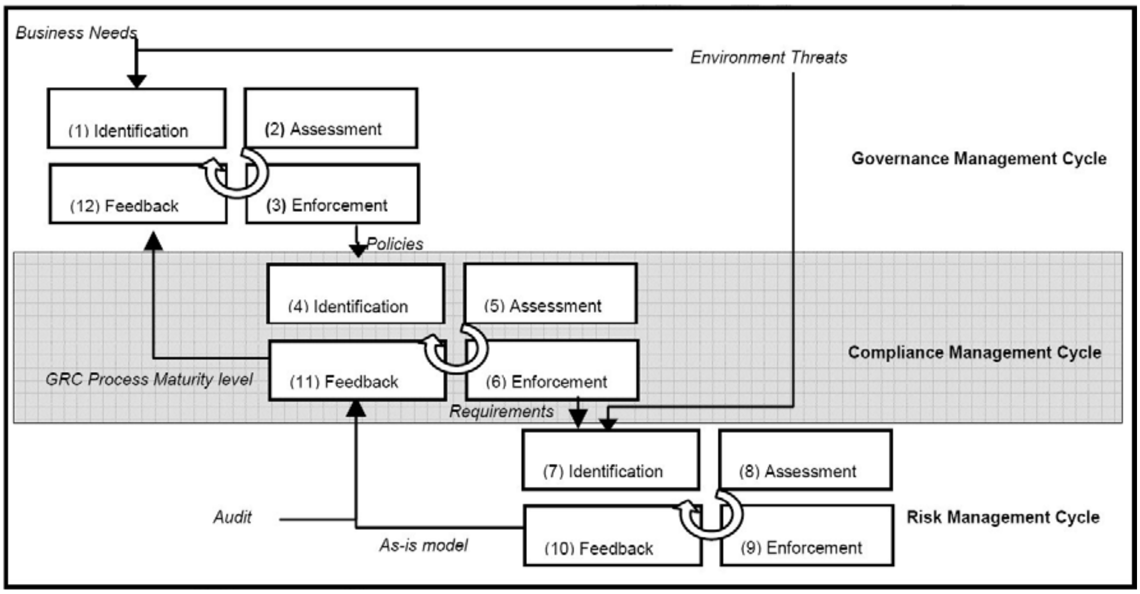


Figure 3.1: IT GRC process: the four-step compliance management cycle is in charge of aligning the Governance and the Risk Management cycles (source: Bonazzi et al. 2008).

Finally the feedback step (step number 11 in figure 3.1) deals with visualization of the gap-analysis, and to do so one can follow the suggestions of Bellamy et al. [18].

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 [200]: 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[239] 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 [163].

- 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.

3.3 Designing a compliance support system (CSS)

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

3.3.1 Problem analysis and our goals

Figure 3.2 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.

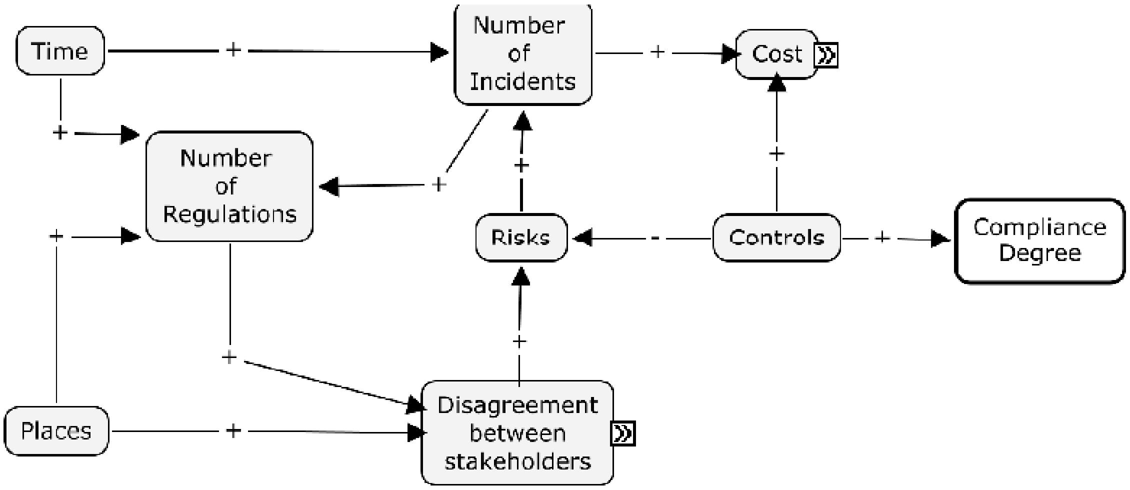


Figure 3.2: Problem Analysis

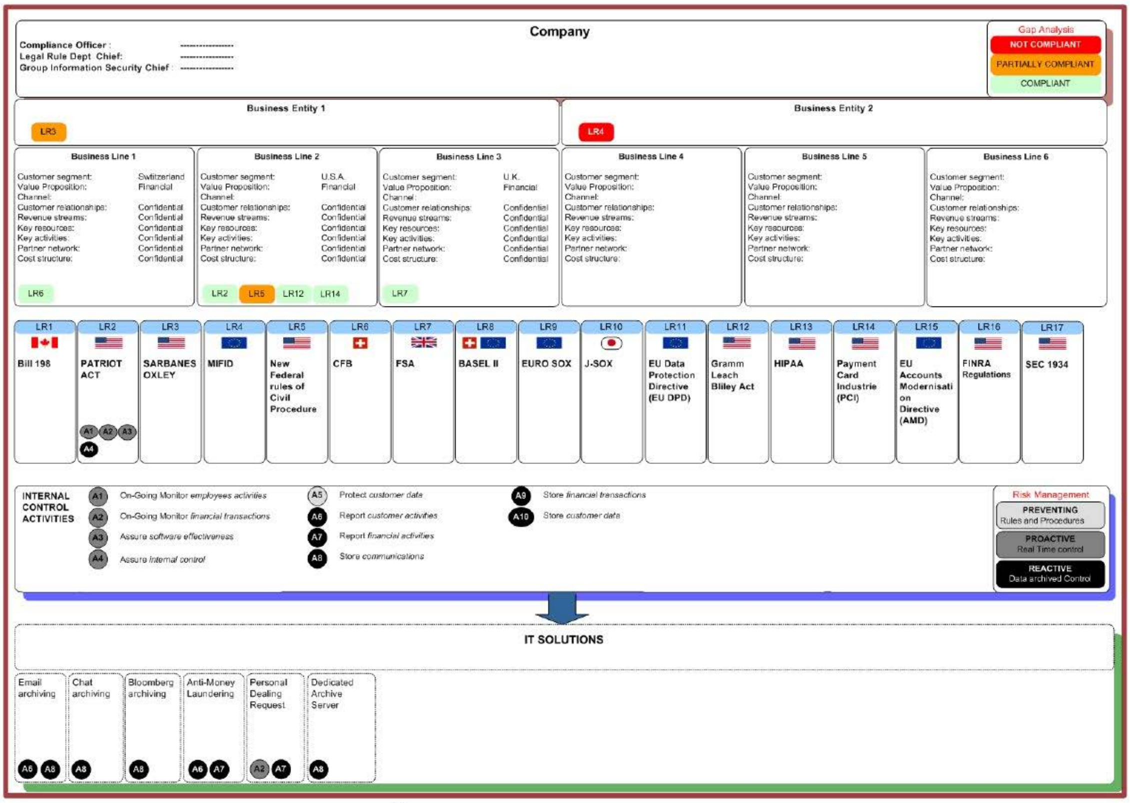
3.3.2 The general design of the artifact

Figure 3.3 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”.



Company

Compliance Officer : ----------------
Legal Rule Dept Chief: ----------------
Group Information Security Chief : ----------------

Gap Analysis
🟥 NOT COMPLIANT
🟧 PARTIALLY COMPLIANT
🟩 COMPLIANT

Business Entity 1
LR3

Business Entity 2
LR4

Business Line 1

Customer segment:	Switzerland
Value Proposition:	Financial
Channel:	
Customer relationships:	Confidential
Revenue streams:	Confidential
Key resources:	Confidential
Key activities:	Confidential
Partner network:	Confidential
Cost structure:	Confidential

LR6

Business Line 2

Customer segment:	U.S.A.
Value Proposition:	Financial
Channel:	
Customer relationships:	Confidential
Revenue streams:	Confidential
Key resources:	Confidential
Key activities:	Confidential
Partner network:	Confidential
Cost structure:	Confidential

LR2 LR5 LR12 LR14

Business Line 3

Customer segment:	U.K.
Value Proposition:	Financial
Channel:	
Customer relationships:	Confidential
Revenue streams:	Confidential
Key resources:	Confidential
Key activities:	Confidential
Partner network:	Confidential
Cost structure:	Confidential

LR7

Business Line 4

Customer segment:
Value Proposition:
Channel:
Customer relationships:
Revenue streams:
Key resources:
Key activities:
Partner network:
Cost structure:

Business Line 5

Customer segment:
Value Proposition:
Channel:
Customer relationships:
Revenue streams:
Key resources:
Key activities:
Partner network:
Cost structure:

Business Line 6

Customer segment:
Value Proposition:
Channel:
Customer relationships:
Revenue streams:
Key resources:
Key activities:
Partner network:
Cost structure:

LR1	LR2	LR3	LR4	LR5	LR6	LR7	LR8	LR9	LR10	LR11	LR12	LR13	LR14	LR15	LR16	LR17
Bill 198	PATRIOT ACT A1 A2 A3 A4	SARBANES OXLEY	MIFID	New Federal rules of Civil Procedure	CFB	FSA	BASEL II	EURO SOX	J-SOX	EU Data Protection Directive (EU DPD)	Gramm Leach Bliley Act	HIPAA	Payment Card Industrie (PCI)	EU Accounts Modernisation Directive (AMD)	FINRA Regulations	SEC 1934

INTERNAL CONTROL ACTIVITIES

A1 On-Going Monitor *employees activities*
A2 On-Going Monitor *financial transactions*
A3 Assure *software effectiveness*
A4 Assure *internal control*
A5 Protect *customer data*
A6 Report *customer activities*
A7 Report *financial activities*
A8 Store *communications*
A9 Store *financial transactions*
A10 Store *customer data*

Risk Management
PREVENTING Rules and Procedures
PROACTIVE Real Time control
REACTIVE Data archived Control

IT SOLUTIONS

Email archiving	Chat archiving	Bloomberg archiving	Anti-Money Laundering	Personal Dealing Request	Dedicated Archive Server
A6 A8	A8	A8	A6 A7	A2 A7	A8

Figure 3.3: The design of the artifact's interface

3.3.3 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 3.4 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 [82]. 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.

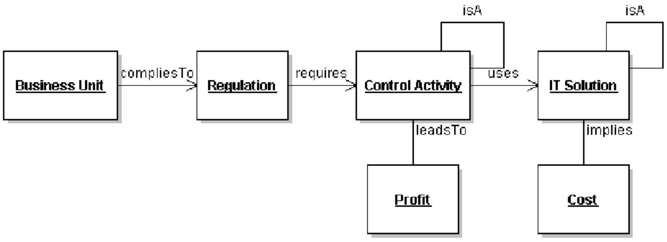


Figure 3.4: Data Objects

We have also defined another object, called "Control Activity", which recalls the idea of "patterns" of Compagna et al. [52], as well as the "legal annotation" of Breux and Anton [33]. 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 [48]. 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 [98]. The associations between data objects follow the viewpoints of the stakeholders. Referring to Bagheri and Ghorbani's [11] 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.

3.3.4 Function of the systems

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.

3.4 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.

3.4.1 Our evaluation criteria

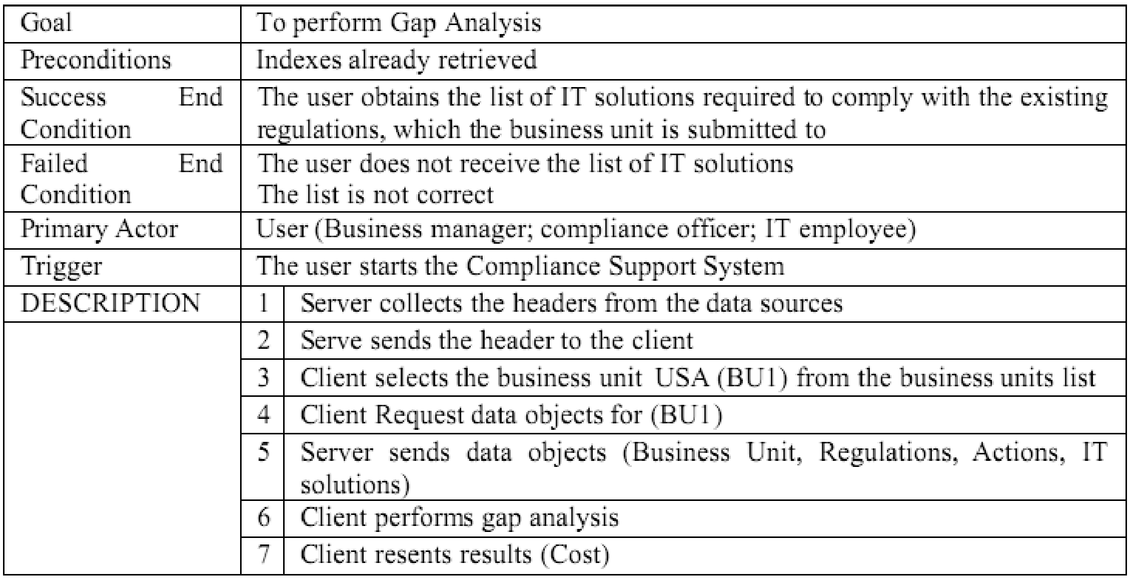
According to our research question, we defined the following set of evaluating criteria, which we wanted to satisfy.

– 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).

3.4.2 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. Figure 3.5 illustrates how we expect the artifact to react in this scenario.

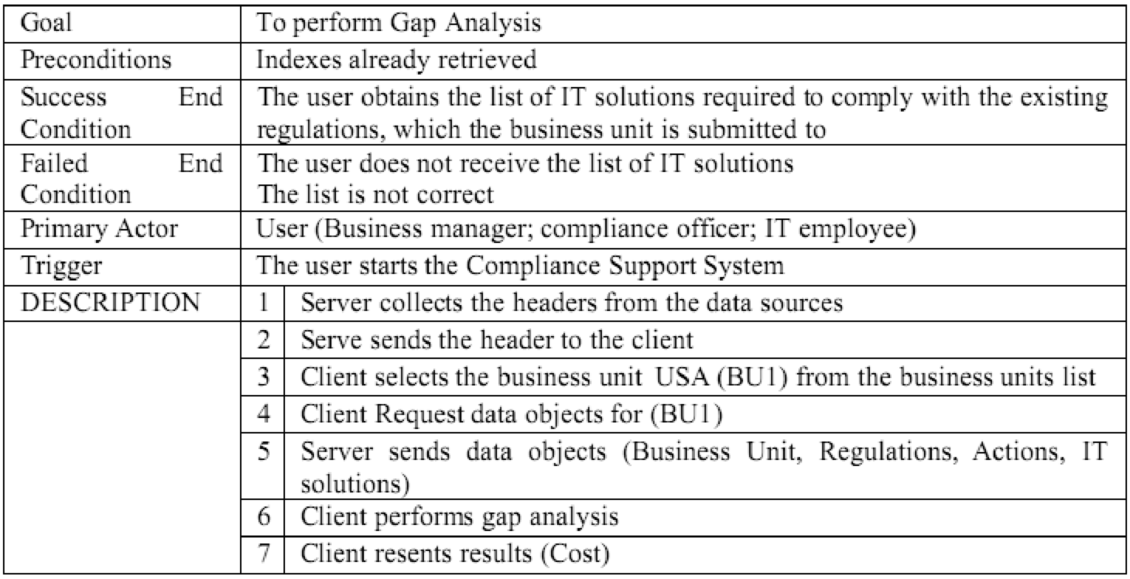


Goal	To perform Gap Analysis	
Preconditions	Indexes already retrieved	
Success End Condition	The user obtains the list of IT solutions required to comply with the existing regulations, which the business unit is submitted to	
Failed End Condition	The user does not receive the list of IT solutions The 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)

Figure 3.5: Performing a gap analysis

3.4.3 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. Figure 3.6 illustrates how we expect the artifact to react in this scenario.

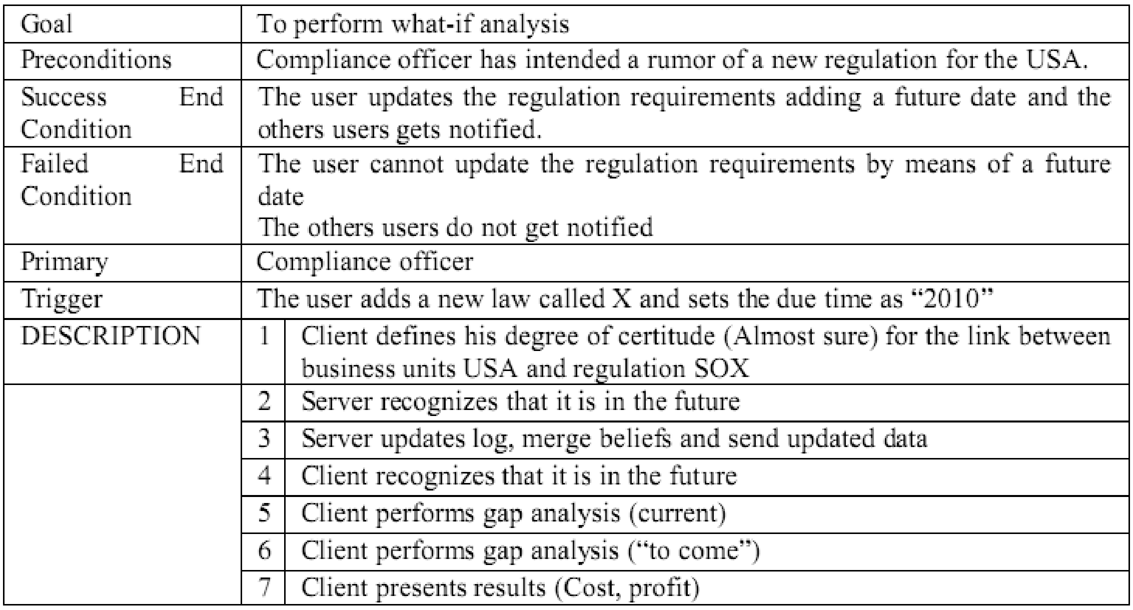


Goal	To perform Gap Analysis	
Preconditions	Indexes already retrieved	
Success End Condition	The user obtains the list of IT solutions required to comply with the existing regulations, which the business unit is submitted to	
Failed End Condition	The user does not receive the list of IT solutions The 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)

Figure 3.6: Adapting regulations requirements

3.4.4 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. Figure 3.7 illustrates how we expect the artifact to react in this scenario.



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)

Figure 3.7: Dealing with future regulations requirements

3.5 Discussion of Potential Findings and Outcomes of the Research

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

3.5.1 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 [239] 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 3.1 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.

3.5.2 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 [161].
- Automatic enforcement. A parallel study in our institute [116] 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.

Chapter 4

IT Governance, Risk & Compliance (GRC) Status Quo and Integration

Abstract

The integration of governance, risk, and compliance (GRC) activities has gained importance over the last years. This paper presents an analysis of the GRC integration efforts in information technology departments of three large enterprises. Action design research is used to organize the research in order to assess IT GRC activities based on a model with five dimensions. By means of semi-structured interviews key findings concerning the status quo of the three IT GRC disciplines, their integration and their relation to GRC on the corporate level are identified and rated. Five key findings explain the main commonalities and differences observed.

4.1 Introduction and motivation

Over the last years the pressure on information technology (IT) managers in enterprises has steadily increased. The auditing profession observes a trend away from the examination of outcomes towards assurance of the processes that produce these outcomes [55]. Hence the growing importance of IT in enabling business processes has shifted the focus of auditors towards information systems. At the same time high-impact regulations such as the Sarbanes-Oxley Act of 2002 (SOx) [53], Basel II [79] and the European directive 2006/43/EC [180], but also crisis-prone markets and governance scandals have created a myriad of new requirements for the governance, risk management, and compliance of companies.

In an attempt to control the increasing complexity, the acronym "GRC" has emerged. It describes an integrated approach to governance, risk management and compliance. When restricted to GRC activities for IT operations, the term "IT GRC" is used [193, 98]. IT

GRC thus comprises IT governance (ITG), IT risk management (ITRM) and IT compliance (ITC). According to ISO/IEC 38500:2008 [125], ITG is “the system by which the current and future use of IT is directed and controlled. [It] involves evaluating and directing the plans for the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.” ITRM in our research is seen as a part of enterprise risk management (ERM), which is “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives” [56]. ITC describes processes to assure the adherence of an organization’s information technologies to laws, regulations, contracts and other obligations [202].

The high interest in the acronym GRC is evident in the growing GRC market [201]. The “Big Four” auditing firms all offer concepts and services for integrated GRC. Dozens of software vendors have developed applications that facilitate GRC management. The competitive pressures and the market’s upside potential have triggered market consolidation [178, 42]. However, all these developments occur almost unnoticed by scientific research [191], especially in regard to IT. For that reason the authors of this paper started to engage in GRC research. According to the research framework of Hevner et al. [109], the relevance of scientific IS research for the targeted environment has to be ensured. The involvement of people, the use of technology, strategies, and processes in the environment have to be considered. So far we hardly know anything about efforts to integrate GRC in IT departments. As research lags behind the industry, an analysis of IT GRC in business practice is a good starting point to catch up. A review of prior research will help outline the research gap in order to formulate a precise research question.

4.2 Prior research

The term GRC and its potentials for integration were first described in 2004 by PricewaterhouseCoopers [188]. For years software vendors, consultancies, and market research were basically the only sources promoting GRC [191]. While the two former mainly publish articles, white papers, and interviews lacking depth, only market research provides more useful documents. Gartner and Forrester Research prepare yearly rankings of GRC software platforms [155, 41]. They also describe frameworks that classify GRC software functionality [40, 156]. However, from the viewpoint of scientific research their reports have several deficits. Firstly they focus on technologies already available and they hardly develop ideas for prospective software. Secondly the details of how the rankings were derived are not published; it is not known if the process applied holds up to scientific standards. Thirdly the independence of the reports is questionable as they need to generate revenues.

More comprehensive and detailed work is provided by the Open Compliance and Ethics Group (OCEG) that bundled the views of industry professionals in a GRC process framework [169] and a blueprint for IT supporting GRC [160, 170]. The frameworks are very extensive, putting much more under the GRC umbrella than the “GRC management”-focused market research companies and software vendors [195]. Unfortunately, the IT blueprint also focuses on software currently available. Another defect of both OCEG frameworks is that they promote a holistic view of GRC but do not really explain how the disciplines can be integrated.

While scientific research has treated the separate topics of (IT) governance, risk management, and compliance in the past, their integration was mostly ignored; the relation of integrated GRC and IT has been examined even less. The ACM Digital Library returns no relevant results that take a comprehensive view of GRC when searched for GRC as an acronym or for "governance, risk, compliance". Sometimes two of the three disciplines were studied superficially [160, 234]. Both sources only talk about ITG and ITC, ignoring the relation to risk management. Thus they are incomplete from the viewpoint of GRC. One of the few scientific papers on GRC software compared the perspectives on GRC software of software vendors, marke research and OCEG, concluding that neither contemporary software nor the frameworks of market research and OCEG are a valid basis for GRC research [195]. Probably the first scientific paper describing integrated GRC, published in 2007, is OCEG-chairman Mitchell's framework for "principled performance" – describing the goal of enterprises to achieve the best possible performance while acting within mandated and voluntary boundaries [158]. The document gives some high-level hints of where integration potentials exist, but it does not delve into detail. Another strategic framework for GRC was suggested by Marekfia and Nissen [151]. The authors do not show the relation of their framework to information technology at all. In 2010 Racz et al. derived a scientific short-definition of GRC by means of a literature review and a validation survey among GRC experts. According to them "GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness" [191]. In further research the same authors merged standards and best practices in a conceptual process model for integrated IT GRC management [193]. Their model has yet to be validated, though.

To sum it up, research has developed a GRC definition; it has started to examine IT GRC processes and it has reviewed GRC software and industry frameworks. In order to further catch up with IT GRC developments in the industry, the analysis of IT GRC in business practice is a consequential next step. With the understanding of the status quo and GRC integration efforts gained in such an analysis, the relevance of further research for the environment can be assured. Therefore this paper addresses the following research question: How is IT GRC performed in large enterprises?

4.3 Methodology

The chosen state-of-the-art methodology is called "action design research" (ADR) [215], an approach recently presented at the Australasian Conference on Information System. It combines design research and action research to enlarge the focus of research on enterprises, helping obtain technological rigor and organizational relevance. Figure 4.1 shows the methodology's four interacting elements. Two guiding principles for problem formulation (1) concern the need to find a balance between theory and practice. The

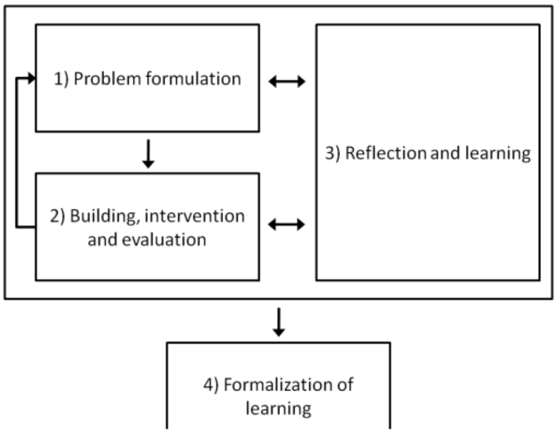
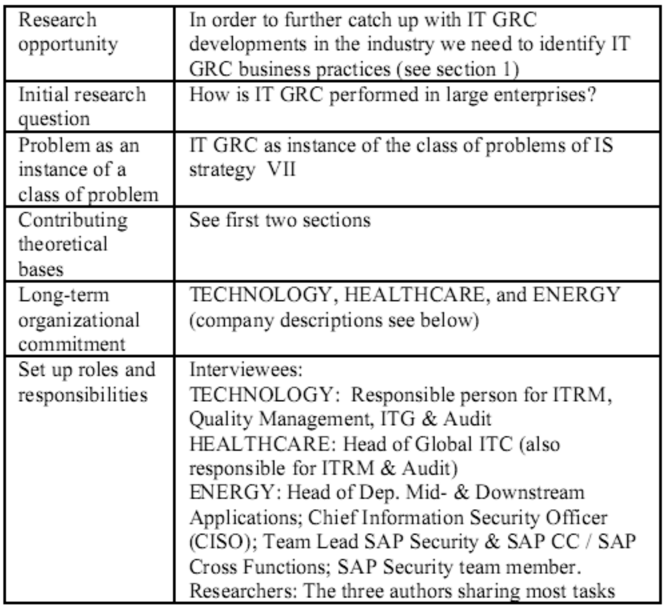

1) Problem formulation
2) Building, intervention and evaluation
3) Reflection and learning
4) Formalization of learning

Figure 4.1: Action Design Research elements (adapted from [215])

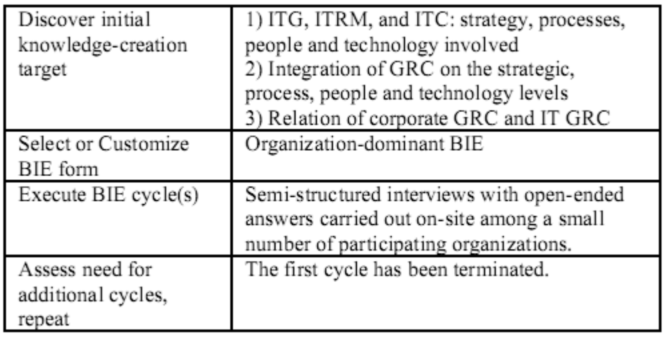
building, intervention and evaluation phase (2) is guided by three principles, which require the close relationship between researchers and practitioners. The third element is dedicated to reflection and learning (3). It should satisfy guided emergence. The last element (4) concerns generalization of the outcomes. Problem formulation is summarized in figure 4.2.



Research opportunity	In order to further catch up with IT GRC developments in the industry we need to identify IT GRC business practices (see section 1)
Initial research question	How is IT GRC performed in large enterprises?
Problem as an instance of a class of problem	IT GRC as instance of the class of problems of IS strategy VII
Contributing theoretical bases	See first two sections
Long-term organizational commitment	TECHNOLOGY, HEALTHCARE, and ENERGY (company descriptions see below)
Set up roles and responsibilities	Interviewees: TECHNOLOGY: Responsible person for ITRM, Quality Management, ITG & Audit HEALTHCARE: Head of Global ITC (also responsible for ITRM & Audit) ENERGY: Head of Dep. Mid- & Downstream Applications; Chief Information Security Officer (CISO); Team Lead SAP Security & SAP CC / SAP Cross Functions; SAP Security team member. Researchers: The three authors sharing most tasks

Figure 4.2: Problem formulation

As mentioned in the table, three companies agreed to take part in the research project: TECHNOLOGY is a global provider of business software and consulting services. Its global IT department employs about 2,000 people, IT employees in business functions not included. For realization of business processes the enterprise has mostly deployed SAP software. HEALTHCARE supplies healthcare products to clients around the world. Its large IT organization provides the IT infrastructure and business support. SAP software is widely used by HEALTHCARE, but they also run business process solutions from several other vendors. ENERGY has most of its staff in Europe, but runs production and exploration activities in many other countries outside of Europe. Its IT department is an own legal entity fully owned by ENERGY's corporate organization. It employs about 550 IT staff and 150 external contractors. IT personnel mainly work at two locations in Europe. 30% of administration tasks supported by IT are SAP applications. The SAP landscape alone has more than 7,000 users. TECHNOLOGY and HEALTHCARE each had a single person respond to all questions, whereas ENERGY organized a meeting with four IT employees. Once a satisfactory formulation of the problem was achieved, the "Building, Intervention, and Evaluation" (BIE) phase started with a discussion of the topics in figure 4.3.



Discover initial knowledge-creation target	1) ITG, ITRM, and ITC: strategy, processes, people and technology involved 2) Integration of GRC on the strategic, process, people and technology levels 3) Relation of corporate GRC and IT GRC
Select or Customize BIE form	Organization-dominant BIE
Execute BIE cycle(s)	Semi-structured interviews with open-ended answers carried out on-site among a small number of participating organizations.
Assess need for additional cycles, repeat	The first cycle has been terminated.

Figure 4.3: Building, Intervention and Evaluation

The artifact we wanted to obtain through answering the research question is a model, i.e. "a description, that is, as a representation of how things are" [150]. As technology is only one of several elements relevant in the model we adopted an organization-dominant rather than IT-dominant BIE form. Semi-structured interviews with open-ended answers were designed. A pre-defined but flexible set of questions guided through the interviews, allowing the interviewer to adapt questions to the situation, to change the question order and to ask new questions if beneficial to the procedure [144]. We designed the questionnaire to hold three question groups: the first group treated ITG, ITRM, and ITC separately, gaining basic information such as definitions, standards followed, personnel involved or technology used for each of the three disciplines. The second group consisted of questions about the integration of IT GRC. We focused on horizontal integration of the three disciplines with each other, not on vertical integration with business processes. Questions concerning the integration of corporate-level GRC with IT GRC formed the third group. We used the frame of reference for research of integrated GRC ([191]; see figure 4.4) for scoping and to give hints about areas of interest. The "operations managed and supported through GRC" in this case are operations of the IT departments. All other elements of the frame were considered in varying details in the questionnaire and in execution of the interviews. We wanted to inquire about all four components (strategy, processes, people and technology), across all three disciplines, and we looked if they were integrated and applied organization-wide and holistically. GRC outcomes and the rules of GRC (internal policies, external regulations and the risk appetite) were only briefly addressed.

The interviews were all conducted by the same person in order to guarantee consistency. They were carried out in two-hour sessions within two months on the sites of participants.

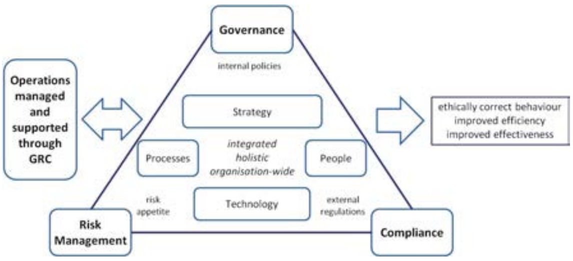


Figure 4.4: Frame of reference for research of integrated GRC

During and after the interview sessions the participants provided relevant documents, presentations and intranet contents that helped answer certain questions more precisely. The answers were analysed and compared, and rated in five dimensions of a model derived from the literature review:

- ITG: the maturity level of the IT governance.
- ITRM: the maturity level of the IT risk management.
- ITC: the maturity level of the IT compliance process.
- ITGRC: the degree of integration among ITG, ITRM and IT GRC.
- GRC-ITGRC: the degree of integration among corporate-level GRC and IT GRC. = Avg(ITG, ITRM, ITC).

For now the dimensions are first-order constructs used to describe all possible ideal types in theory [70]. All dimensions can have one of three possible values representing the maturity level of their processes using the framework of the IT policy compliance group [98]: “high” for a score of 4 or higher out of 5, “low” for a score below 2 and “medium” otherwise. The values of ITGRC and GRC- ITGRC integration can never be better than the average of the ITG, ITRM and ITC values (ITGRC ¡= Avg(ITG, ITRM, ITC; GRC-ITGRC ¡= Avg(ITG, ITRM, ITC).

In the following section we present the result of our first BIE iteration.

4.4 Key findings

Five key findings shall help gain an idea of the interview contents and important notions that influenced consequent research stages.

4.4.1 IT Governance varies strongly in enterprises.

In theory there are two principal perspectives on GRC [205, 142]. One focuses on structural characteristics, e.g. decision and accountability such as the ITG model of Weill and Ross that suggests five decision domains [250]. The second ITG perspective emphasizes process mechanisms, such as controls and risk management. Not surprisingly a mix of the two views was observed in all three companies.

TECHNOLOGY has a strongly formalized, requirements-oriented understanding of IT governance. Its global IT governance framework collects requirements from national and international standards (such as ISO/IEC 27001 [124], BS 25999 [34, 35] and ISO 9001 [123]), laws and regulations (e.g. SOx, insider and tax regulations, data protection laws), and supporting best practices (COBIT [122], ITIL [171], and PMBOK for project management [121]). The framework "assures an effective business/IT interface and enables careful coordination of all IT activities to drive standardization of IT processes and the IT technology landscape." A three-step ITG process was designed: it consists of identifying and monitoring standards, laws and best practices (1), reviewing and approving the proposal for changes in the ITG framework (2), and updating the framework (3). The process is triggered ad-hoc whenever changes in laws or standards or new risks emerge. Through the framework the whole IT organization shares a common understanding of ITG. ITG is further subdivided into IT security governance, governance of enterprise architecture and vendor management governance (the two latter better embodying the decision perspective), all taken care of by different teams but aligned through the common framework.

HEALTHCARE defines "IT process governance" within IT service management (ITSM), established to "define and ensure process excellence in IT". Key objectives are the establishment of a harmonized ITSM framework, the implementation of service level agreement and best practices, the definition of key performance indicators and service level objectives, the fulfillment of regulatory requirements and increasing the efficiency of IT operations. A common understanding is shared by IT personnel through this definition as well as existing standard architectures and process definitions; the latter include COBIT and ITIL. An ITG function is defined on the group and divisional level. HEALTHCARE currently discusses if the divisional and group-level functions should be merged.

ENERGY focuses on three deliverables of ITG: the maturity of services provided, business partner satisfaction, and project management effectiveness. The company uses governance to "address the right behavior to achieve corporate goals". A triangle of the CIO representing the group's IT interests, the internal IT supplier of IT services and projects, and business operations defining the IT demand ensures alignment and contribution to business value. The CIO is accountable for all facets of ITG, sharing responsibility and support tasks with business unit IT leads and division IT leads, also involving various committees. Figure 4.5 highlights the building blocks of ENERGY's IT governance.

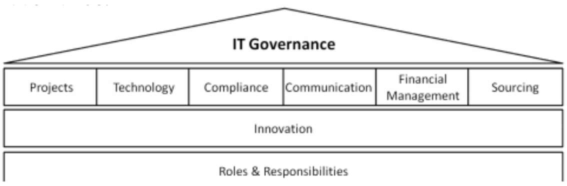


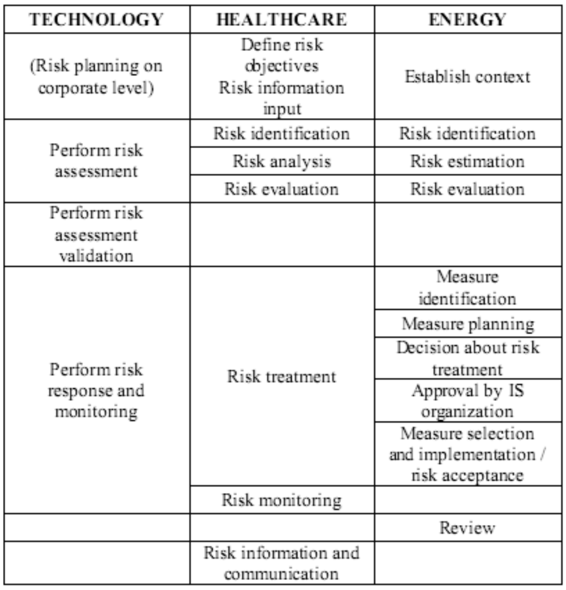
Figure 4.5: ENERGY's IT governance building blocks

None of the companies currently uses dedicated ITG software. In summary they have different perspectives on IT governance: from a strongly formalized standards-oriented process view at TECHNOLOGY (ITGT = "high") ; over less formal ITG embodied in the IT organization's culture and processes (ITGH = "medium"); to a perspective where governance is clearly formalized, but focusing more on responsibilities and goals, centered on the CIO (ITGE = "high").

4.4.2 IT risk management follows established frameworks.

Even though different wording is used for process categories, in general ITRM in the three companies hardly differs (see figure 4.6). The ITRM process typically starts with a planning phase in which risk objectives are set. Risk identification and assessment are carried out before risk response measures are selected and implemented. The risks are monitored and reported to relevant stakeholders.

Minor differences exist in the point in time of risk validation and in the formalization of reviews, monitoring and reporting. The only notable big difference is found on lower process levels of the risk assessment procedure. TECHNOLOGY classifies risk using five rough ranges of financial impact and probability. HEALTHCARE calculates the impact of each risk more precisely following the COSO ERM approach but also using ranges. ENERGY uses a software product called "CRISAM" for implementation of ITRM, which recalls the ISO 270005 methodology; CRISAM does not use probabilities at all, relying on the comparison of actual impacts with target values instead.



TECHNOLOGY	HEALTHCARE	ENERGY
(Risk planning on corporate level)	Define risk objectives Risk information input	Establish context
Perform risk assessment	Risk identification	Risk identification
	Risk analysis	Risk estimation
	Risk evaluation	Risk evaluation
Perform risk assessment validation		
Perform risk response and monitoring	Risk treatment	Measure identification
		Measure planning
		Decision about risk treatment
		Approval by IS organization
		Measure selection and implementation / risk acceptance
	Risk monitoring	
		Review
	Risk information and communication	

Figure 4.6: High-Level IT Risk Management Processes

In summary we can say that ITRM of all companies shows high maturity (ITRMT = ITRMH = ITRME = "high").

4.4.3 IT Compliance in companies is mature.

TECHNOLOGY sees IT compliance as part of IT security. SOx compliance dominates, but other standards from the ITG framework are also assessed. The main compliance process for SOx consists of four phases: control documentation, control design assessment, control effectiveness testing, and corporate sign-off. SOx compliance is checked twice a year. ISO 9001, ISO/IEC 27000, and BS 25999 compliance are checked yearly. Audits are coordinated by means of an audit map. TECHNOLOGY has 90 automated IT controls in place that are managed through a deprecated version of a tool for automated IT controls. The main ITC management tool is a giant spreadsheet based on an Access database that is used in ITRM as well as for ITC.

For compliance assessments at HEALTHCARE, IT topics (such as "SAP") are subdivided into compliance topics (such as IT security) and linked to "reasons" (e.g. external policies and laws) and controls. Once a year an assessment sheet is sent to all sites that have to rate their maturity level for each control. The team of our interviewee then compares the sheet to the results of the last evaluation. The outcome and some other factors influence the decision if an audit is carried out. Audits are planned once a year; there are 14 audit types (e.g. site audit, ITG audit) carried out at different intervals. An Access database with reminder functionality saves and helps track all audit actions. The database and the spreadsheets are about to be superseded by a standard software audit tool allowing for direct data input, supporting audit planning and field work, and pushing relevant information to users in the company's portal.

ENERGY does not have a defined stand-alone ITC process, as ITC activities are integrated with ITRM. These integrated activities evolve around the ISO/IEC 27000 row standards, recommendations of the Business Continuity Institute and the Statement on Auditing Standards 70 [4]. The CIO office constantly carries out IT audits. Software from Tripwire supports compliance management, while applications of other vendors ensure prevention, monitoring and detection of compliance. SAP Access Control manages access and authorization controls.

In summary we can assess that ITCT = ITCH = "high", and ITCE = "medium" due to lower formalization.

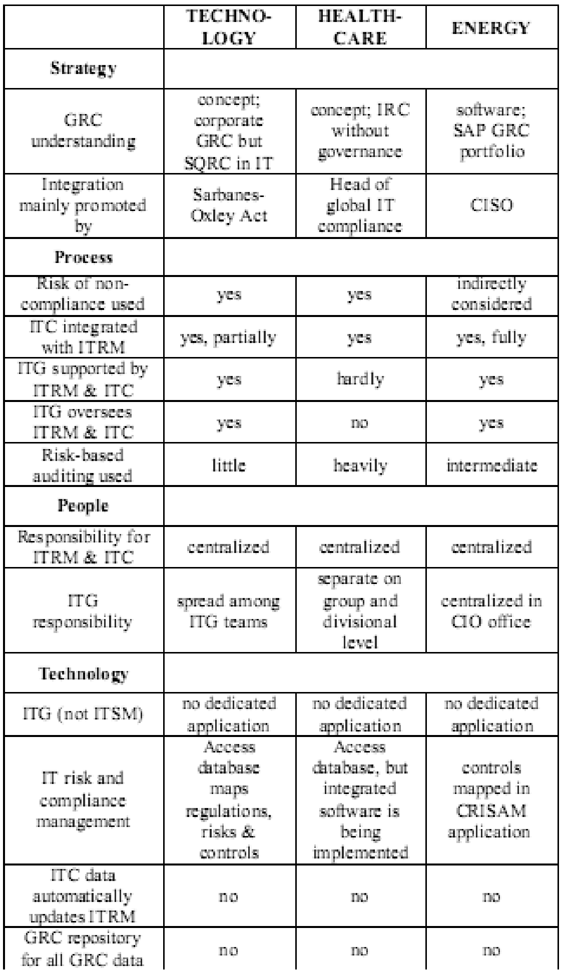
4.4.4 IT GRC disciplines are integrated in manifold ways.

Our study revealed many ways in which the companies have started to integrate IT GRC activities. Some of the taken measures are exemplarily described in figure 4.7 and in the subsequent paragraphs.

The differing understanding of GRC is notable; while GRC integration efforts can be observed in all companies, the acronym is not always used to describe it. Security, Quality, Risk and Compliance form "SQRC" at TECHNOLOGY, HEALTHCARE speaks of integrated risk and compliance ("IRC").

On the process level the integration of ITC with ITRM is far advanced, especially at ENERGY, where ITC is carried out as part of ITRM similar to recommendations from theory [193]. The consideration of the risk of non-compliance and the use of risk-based auditing are other means of ITC-ITRM integration. The two-fold relation of governance and the other two disciplines, with ITG governing ITRM and ITC and at the same time being supported by them e.g. through data provision for decisions [193], existed in two companies but was weak at HEALTHCARE due to its generally lower ITG formalization.

On the technology level, integration opportunities have not been leveraged much. The giant spreadsheet TECHNOLOGY uses is generated through a Microsoft Access database in



	TECHNOLOGY	HEALTHCARE	ENERGY
Strategy			
GRC understanding	concept; corporate GRC but SQRC in IT	concept; IRC without governance	software; SAP GRC portfolio
Integration mainly promoted by	Sarbanes-Oxley Act	Head of global IT compliance	CISO
Process			
Risk of non-compliance used	yes	yes	indirectly considered
ITC integrated with ITRM	yes, partially	yes	yes, fully
ITG supported by ITRM & ITC	yes	hardly	yes
ITG oversees ITRM & ITC	yes	no	yes
Risk-based auditing used	little	heavily	intermediate
People			
Responsibility for ITRM & ITC	centralized	centralized	centralized
ITG responsibility	spread among ITG teams	separate on group and divisional level	centralized in CIO office
Technology			
ITG (not ITSM)	no dedicated application	no dedicated application	no dedicated application
IT risk and compliance management	Access database maps regulations, risks & controls	Access database, but integrated software is being implemented	controls mapped in CRISAM application
ITC data automatically updates ITRM	no	no	no
GRC repository for all GRC data	no	no	no

Figure 4.7: IT GRC integration

which assets, control objectives, risks and controls are stored and tracked. The spreadsheet enables a holistic view on IT GRC management. Consistency is ensured through a walkthrough with the different stakeholders and is maintained by the ITRM team. However this manual process is very tedious, causing our interviewee to wish for a software update to the latest release of SAP GRC risk management. As of now, operational risk management software is used on the corporate level for strategic risks and to enter high-level IT risks, but that software is not used for all operational ITRM activities (e.g. due to missing specific ITRM data fields). A deployed internal controls application has insufficient reporting capabilities and it cannot be integrated with the Access database to enable automated control status updates.

HEALTHCARE is in the process of replacing its current solution involving Microsoft Access, Excel and emails, supported by a balanced scorecard showing existing and upcoming risks, with an integrated IT risk and compliance solution. The results of risk and compliance assessments will be entered directly into the application by system owners, site managers and other relevant personnel. The mapping of risks to controls, regulations or assets as done today will still be enabled by the software. Reporting capabilities are integrated. An integrated multi-regulatory compliance framework will help reduce compliance complexity and it will prevent duplicate efforts.

ENERGY has deployed software from Tripwire for compliance management, while applications of several other vendors ensure prevention, monitoring and detection of compliance. SAP-BO Access Control is used to manage access and authorization controls, but this is more of an operational tool and thus it is not in the scope of IT GRC management. The risk management tool "CRISAM" has helped standardize ITRM, but the additional automated control and monitoring solutions are disconnected. While ENERGY is not depending on spreadsheets, its IT GRC management activities are not supported by a comprehensive solution.

The integration maturity of all three companies can be described as "medium", as integration can be observed especially on the process and people levels, but technology integration lags behind.

4.4.5 Efforts to align and integrate IT GRC with corporate-level GRC have been undertaken.

This finding refers to business-IT-alignment (see Chen at al. [46]), as the concept of integrated GRC suggests integration of all GRC activities of an organization – not only those of the IT department. TECHNOLOGY sticks out from an organizational point of view having established a global corporate GRC function, aligning GRC activities enterprise-wide, leading and helping business lines and supporting functions such as IT adhere to GRC requirements.

However, TECHNOLOGY's corporate governance codex was not used in the definition of its ITG framework. ITG at HEALTHCARE was developed in accordance with the corporate governance requirements, but does not refer to it in its key objectives. At ENERGY corporate governance influenced the creation of its ITG model, and the role of the CIO in corporate governance also links it to ITG.

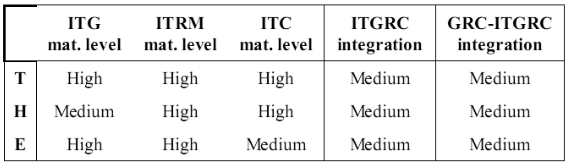
The relation of corporate risk management to ITRM is similar for HEALTHCARE and TECHNOLOGY, but differs at ENERGY. All three use software applications for strategic risk management. A small number of aggregated, material risks from ITRM are entered into the corporate software. Facts and s are translated into the ERM ontology to guarantee comparability with other ERM data. Personnel responsible for ERM rely on the data input from IT. The risk management process definitions in the companies differ. At ENERGY different processes (with similar activities) are used to carry out ITRM and ERM. TECHNOLOGY and HEALTHCARE, in contrast, use a single policy for all types of risk including IT risk. Recent notions in research go even further, questioning the need for separate ITRM frameworks [194]. HEALTHCARE has already harmonized corporate and ITRM processes, and now discusses if the execution of the risk management processes should also be synchronized. That way, group-level risks would be broken down to lower levels, and other risks on these lower levels would be identified in the same breath.

ITC is connected to corporate compliance in several ways. Only a part of the myriad of GRC requirements is directed towards IT operations. Thus processes have to be examined end-to-end. The SOx process at TECHNOLOGY, for example, is led by the corporate GRC function; the IT organization is aligned with and engaged in the corporate SOx process. At HEALTHCARE, internal controls for financial reporting are audited by IT and by the finance department. Due to its role as an enabler of business, IT is often just one of several parties involved in a compliance procedure. Moreover companies have corporate internal audit teams that audit all parts of the enterprise, including IT. That way and through sign-offs across hierarchy levels organizational integration of compliance is established.

Lastly integration aspects exist on the technology level. Automated controls provided by IT not only monitor IT-specific processes, but also business operations supported by IT through the application of business rules. TECHNOLOGY's automated control application is used in the SOx process, both by corporate GRC and by IT. But compliance technology integration at the three companies hardly surpasses IT controls. For example, TECHNOLOGY uses a central company-wide tool combining all strategic and operative risks throughout all business functions including the IT control side; but for the mapping of assets to risks and controls it had to deploy a separate Access database. ENERGY and HEALTHCARE do not have a central tool in place that stores all compliance-relevant data (standards, audit results, logs, control information...). HEALTHCARE is currently pondering the introduction of such a tool. Due to the low process automation, the classification of the companies is as follows: GRC-ITGRCT = GRC-ITGRCH = GRC-ITGRCE = "medium".

4.5 Classyfing IT-GRC maturity

Although it is too soon to formalize our results, we intend here to draft a first step in that sense. This is mostly due to the sake of clarity and only in part to allow for judgement of our preliminary statements. The five rating dimensions compose a model (figure 4.8) coming in the shape of a classification of IT GRC maturity, the three lines representing the values observed in the three companies. The observed patterns can be understood as "complex constructs that can be used to represent holistic configurations of multiple unidimensional constructs" [70].



	ITG mat. level	ITRM mat. level	ITC mat. level	ITGRC integration	GRC-ITGRC integration
T	High	High	High	Medium	Medium
H	Medium	High	High	Medium	Medium
E	High	High	Medium	Medium	Medium

Figure 4.8: Use of the classification with our three cases

4.6 Reflection and learning

In this section we present the third step of ADR, reflecting on what we have learned so far. An assessment of this study with the ADR principles is presented in figure 4.9.

Reflecting on design and re-design during the project, we mention that the artefact originally evolved from a simple 2x2 matrix assessing degrees of process formalization and process automation towards a more complete typology. This was the result of the interaction with experts and the incremental acknowledgement of previous researches in the existing IS strategy literature.

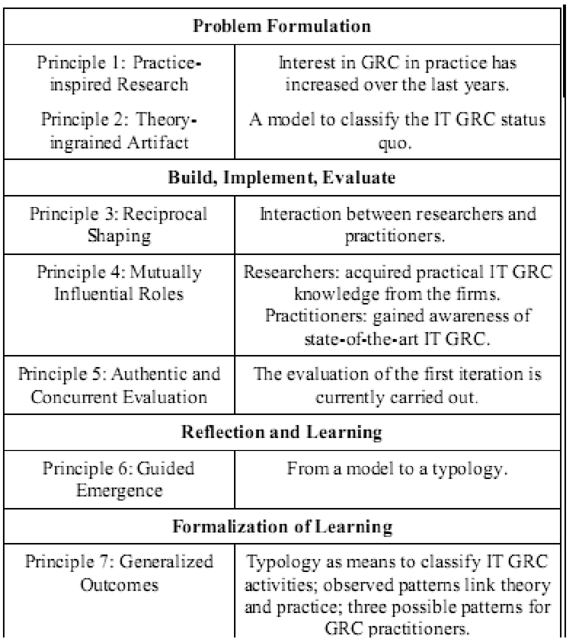
We answered our research question by presenting the status quo of IT GRC activities in three large enterprises. Integration efforts concerning the three disciplines and integration of IT GRC with corporate-level GRC were identified. For the three companies a largely undiscovered potential for further integration seems to lie in process automation through application of integrated software solutions. New theory can build on the results to increase the likelihood of its relevance, addressing the patterns that have been left behind in this study.

Naturally some points of critique can be directed to the methodology applied. Firstly, the examination of three companies is not representative. But at least it gives impressions of IT GRC in three different industries. Considering the variety found in the companies' IT GRC processes, the findings are a satisfying result for an explorative study. Secondly, it is hard to judge in how far the interviewees' answers actually reflect the reality in their companies. For instance, are policies really adhered to? Interviewee's might not exactly know the answer, or they might tend to draw a polished picture of their areas of responsibility. A deeper analysis through witnessing processes at execution could have avoided this deficit. Thirdly, in hindsight we would have liked to know more about the GRC technology used. Looking at spreadsheets such as the risk-controls mapping turned out to be very helpful in understanding the contents of certain processes. However, software applications are too complex to be quickly grasped, and in the interviews there was no time for demonstration. We thus had to rely on vendors' tool descriptions. A more detailed question catalogue about software functionality and its use could have helped gain more insights.

4.7 Conclusion: formalization of learning

In step four of the ADR process we formalize our learning to develop general solution concepts. The research at hand shows that IT GRC integration efforts have already been undertaken in large enterprises in various ways. The key findings highlight commonalities and differences in how the separate disciplines and their integration are addressed, which is not only important for our ADR project, but for other researchers and practitioners as well. Research can build on the tactical view of GRC provided. Practitioners can use our ideal types to define and improve their IT GRC, following the practices presented and trying to surpass them where weaknesses were observed, especially in the use of GRC software applications for better integration.

In future research we will continue to use the ADR methodology, trying to dig deeper in the area of software requirements for integrated GRC platforms in order to propose a technology reference model for integrated IT GRC management.



Problem Formulation	
Principle 1: Practice-inspired Research	Interest in GRC in practice has increased over the last years.
Principle 2: Theory-ingrained Artifact	A model to classify the IT GRC status quo.
Build, Implement, Evaluate	
Principle 3: Reciprocal Shaping	Interaction between researchers and practitioners.
Principle 4: Mutually Influential Roles	Researchers: acquired practical IT GRC knowledge from the firms. Practitioners: gained awareness of state-of-the-art IT GRC.
Principle 5: Authentic and Concurrent Evaluation	The evaluation of the first iteration is currently carried out.
Reflection and Learning	
Principle 6: Guided Emergence	From a model to a typology.
Formalization of Learning	
Principle 7: Generalized Outcomes	Typology as means to classify IT GRC activities; observed patterns link theory and practice; three possible patterns for GRC practitioners.

Figure 4.9: Adehrence to ADR principles

Chapter 5

Respecting the deal: Economically sustainable management of open innovation among co-opeting companies

Abstract

Platforms like eBay allow product seekers and providers to meet and exchange goods. On eBay, consumers can return a product if it does not correspond to expectations; eBay is the third-party firm in charge of assuring that the agreement among seekers and providers will be respected. Who provides the same service for what concerns open innovation, where specifications might not fully defined? This paper describes the business model of an organizational structure to support the elicitation and respect of agreements among agents, who have conflicting interests but that gain from cooperating together. Extending previous studies, our business model takes into account the economic dimensions concerning the needs of knowledge share and mutual control to allow a third-party to sustainably reinforce trust among untrusted partners and to lower their overall relational risk.

5.1 Introduction

This paper deals with co-opetition in open innovation. Open innovation is innovation done outside the company [49], whereas co-opetition occurs when two competitors cooperate on a specific project. Co-opetition can be defined by means of five components: players, added values, rules, tactics and scope [32].

Companies trying to align their strategic intents for cooperation usually face problems of coordination. It is important that each partner's promises will be honoured, i.e. that partners are self-committing. If those companies are competing their lack of common knowledge leads to asymmetry of information and that does not allow for complete trust among them. When that happens the promise done by one partner needs to be honoured, i.e. it is self-committing, and hoped to be believed by the other partner, i.e. it is self-signalling [241]. A trivial example taken from Birchler and Butler [21] could illustrate this situation: a person bringing wine to a dinner (red or white) with a second person cooking the meal (meat or fish). There are two suitable options exploiting the complementarities of the two assets (red wine-meat and white wine-fish), and players are assumed to be neutral in respect to them. Hence, the first person can propose to eat meat and drink red wine, knowing that if the second person agrees to cook meat that he will have no reason to cheat and to bring white wine. Let us assume that the first person prefers red wine, whereas the second person likes fish. Thus the players' assets are substitutes, meaning that either they drink red wine (and they should eat meat) or they eat fish (and drink white wine). In this case, the first person can propose that they eat meat and drink red wine for dinner and that they eat fish and drink white wine on the following dinner; however, that will work only if the second person believes that the first one will honour the promises (i.e. there will be compliance).

Our contention is that co-opetition works for projects where there is a high risk of failure, which a single company is not ready to stand, and where there is a promise of high potential returns for the company to be satisfied even if it receives only a part of it. According to Wagner and Layton [246], there are two kinds of risk: unrewarded, which is a cost to be paid in advance to enter the game, and rewarded, which is the promise of potential returns. On the one hand, co-opetition aims at share the unrewarded risk among partners. On the other hand, this form of partnership requires high efforts for coordination that lead to costs of communication among partners and of control against cheating. Such costs are also known as transaction costs and are reduced when there is trust among allied companies. This can be achieved by giving proof of compliance, which it is here defined in a broader sense as the definition of the objectives of the partnership, the assessment of the failure risk and the enforcement of a set of controls. i According to what said so far this study proposes a framework to achieve the best trade-off between trust and control in order to achieve confidence at a minimum cost. A large amount of literature has focused on information technologies automatically negotiating among enterprises; hence, the focus here is on risk management and compliance. A viable tactic should be to define rules that would shape the alliance in a way that does not reward cheating [135]. In this sense, Hagel [100] suggests using the shared platform to shape the information exchanges among companies. Such a platform can be considered as a critical resource for a third-party enterprise in charge of the coordination among co-opeting companies. Thus, our goal is to sketch the business model of such third-party enterprises, answering the following research question:

Which are the business model components of a third-party enterprise in charge of risk management among co-opeting companies performing open innovation?

This question is addressed using a design science methodology [109]. We follow the guidelines of Gregor and Jones [96] to develop a conceptual model for risk management among co-opeting agents. A conceptual model is defined by March and Smith [150] as a representation of how things are, whose concern is utility, not truth. Such model gives the theoretical ground for the set of business model prescriptions for a trusted third-party, which is presented later in two sections of this paper.

Such guidelines have still to be tested extensively, and for this purpose we illustrate an example of such test using second-hand data from the Innocentive case to give a hint of what we expect to obtain. Innocentive is an independent intermediary, which allows companies to list their innovation challenges and to seek for a solution among a crowd of potential solvers. For example if a drilling company might be looking for an innovative way to drill in special terrain conditions, Innocentive lets the drilling company post its innovation challenge on their website. This way the drilling company can access the knowledge of the thousands of worldwide experts enrolled in the Innocentive website. In recent years Innocentive has been exploring new ways to allow different solvers to gather together for a limited amount of time to solve a challenge. We consider Innocentive a good example to test the representative power of a model to help managing co-opeting agents.

The rest of this paper is organized as follows. Section 2 provides a brief introduction to co-opetition as a hybrid business strategy comprising competition and cooperation, providing theoretical frameworks on coordination and control. Section 3 introduces design research in information systems as the chosen methodology and the business model ontology (BMO) as the conceptual framework to develop the business model. Section 4 describes the proposed business model for a third-party, whereas section 5 lists some testable propositions to falsify the underlying theory of our business model. In section 6 we illustrate how to use our business model pattern using the example of Innocentive. The conclusion of the paper finds place in section 7.

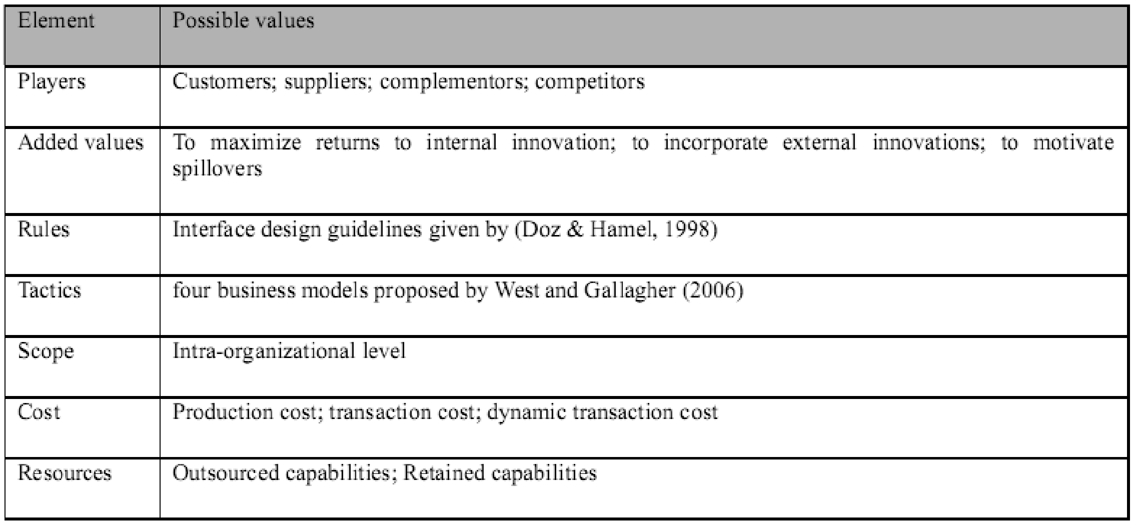
5.2 Coopetition

This section elaborates on co-opetition as an emerging concept in the field of strategy. To obtain insights into this hybrid form of strategy, the existing literature on alliance management is combined with concepts from the risk management and compliance literature. Adopting a systems perspective, a firm can be viewed as an open system interacting with entities in its environment. In order to maintain its existence in a specific context (i.e. viability), a firm has to regulate, optimize and continuously improve its internal operations and to manage its relationships with the external entities [17]. Such interactions appear in two basic ways: cooperation to exchange resources [104, 83] and competition to acquire/maintain customers [186] and resources [210]. In various business settings, firms compete and cooperate at the same time to achieve both advantages and viability. This hybrid form of strategy comprising simultaneous cooperation and competition is labelled co-opetition in the strategy literature [32]. In effect, co-opetition is a common attribute of all systems ranging from firms to living species. Evidence from systems theory suggests that any strong association among systems, be it competitive or cooperative, is doomed to depletion [251]. The rest of the section outlines and briefly elaborates on the theoretical insights that can contribute to our understanding of co-opetition.

5.2.1 Theoretical frameworks for co-opetition

The study of cooperation and competition has been a topic of continuing interest in a variety of disciplines ranging from biology to political science and business strategy

[77]. Various theoretical frameworks can be employed to shed light on the aspects of this phenomenon, but this paper limits itself to business strategy [134]. Therefore we ground our statements into game theory, which describes the interaction among agents, transaction cost theory, which suggests the best way to structure such interactions, and resource-based theory, which analyses the gain from pooling agents' resources together. Evidences from game theory suggest that in the long run cooperation emerges as the evolutionarily stable strategy among competing players. Axelrod [10] suggests that in the Prisoner's Dilemma game, the players who pursue a co-opetitive strategy gain a higher pay-off as compared to those who play with a competitive or a cooperative strategy. A co-opetition game in open innovation can be described using five components (players, added values, rules, tactics and scope) suggested by Nalebuff and Branderburger [163], to which we add two additional elements, i.e. "cost" and "resources", which we derive from transaction cost theory and resource-based theory. The seven elements are listed in 5.1 and described in the rest of this paragraph.



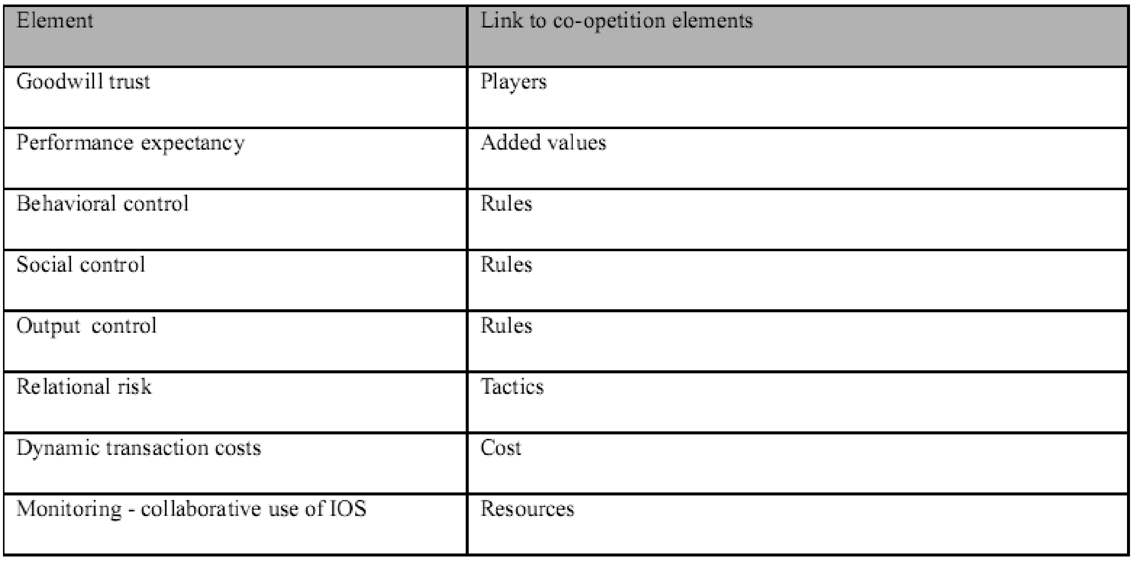
Element	Possible values
Players	Customers; suppliers; complementors; competitors
Added values	To maximize returns to internal innovation; to incorporate external innovations; to motivate spillovers
Rules	Interface design guidelines given by (Doz & Hamel, 1998)
Tactics	four business models proposed by West and Gallagher (2006)
Scope	Intra-organizational level
Cost	Production cost; transaction cost; dynamic transaction cost
Resources	Outsourced capabilities; Retained capabilities

Figure 5.1: Elements of co-opetition framework

Four key role players relate to the main company, which can take part in open innovation: customers, suppliers, complementors and competitors [163]. On what concerns added values West and Gallegher [253] refer to expectancy theory to find the reasons pushing enterprises to contribute in open source software developments. The assessment of the added values for companies raises two issues, that is, how to calculate such value and how to increase it. Simard and West [221] propose a set of metrics, whereas West and Gallegher list three major goals of open innovation: to maximize returns to internal innovation, to incorporate external innovations and to motivate spillovers. The rules in this kind of game deal with the risk of lack of compliance. The risk of wrong coordination between companies [253] is addressed by the design of an interface between companies [72]. Referring to tactics for open innovation, Doz and Hamel [72] assess the shift in the kind of relationship between companies, whereas West and Gallagher [253] describe four business models used by software companies to capitalize their contributions to open sources programs. On the matter of scope, open innovation can be studied at the intra-organizational and firm level as well as at the dyad (i.e. two companies) and inter-organizational level [242]. Our work considers a network of companies, which deal with each other. In this sense legal boundaries are hard to be defined, since different business units in the same enterprise could be submitted to different regulations and deal with each other by means of internal service level agreements. Transaction cost economics (TCE) identifies two types of costs associated with the economic exchanges [256]: production cost and transaction cost. Production cost is defined here as the actual cost of the product or the service; transaction cost includes the extra costs associated with an economic exchange that go beyond the production cost. Such costs include the cost of searching and selecting a product or a service as well as the cost of drafting and enforcing a contract. TCE asserts that a firm should acquire a product, a service or a resource externally only when the production and transaction costs are lower than those of producing it internally [257]. Furthermore, it hypothesizes that higher uncertainty, frequency of transactions, and specificity of the assets result in higher risk of opportunism and consequently higher transaction costs associated with the exchange of the good, service or resource [258]. Based on insights from TCE, co-opetition is a risky business with a higher level of uncertainty than cooperation between non-competitors. This uncertainty leads to higher risk of opportunism, which it is here defined as relational risk that leads to high transaction costs. If two co-opeting companies use a trusted third party to perform the transaction, then the third party will have to manage continuous unilateral interactions with the two companies. Thus, in the long term its main cost would be dynamic transaction costs, defined as the costs of persuading, negotiating and coordinating with, and teaching others [139]. On what concerns resources, resource-based theory consider a firm as an open system for sustainable value creation and distribution. Derived from resource-based theory the competence-based management (CBM) holds that competition and cooperation between firms occur to attract/retain customers, resources and capabilities. Resources include anything tangible or intangible that could be useful to a firm in developing and realizing products to create economic value in its product markets. Capabilities, on the other hand, are repeatable patterns of action for coordinating resources in processes for value creation. Resources and capabilities can reside both within the boundary of firm (firm-specific) and in the firm's environment (firm-addressable). Thus, a third-party enterprise may rely on resource or capability inputs from entities in their external environment that could be their market competitors to sustain the value creation and distribution processes. In this sense, the reader can refer to the managerial, business and technical core capabilities that an enterprise should have to coordinate a set of competing companies in its supply chain [126, 58].

5.2.2 Theoretical frameworks for risk management and compliance in co-opetition

Figure 5.2 presents the elements described in this paragraph, and their link to co-opetition elements. We extend the game theory framework previously presented by defining relational risk as the risk that a partner may fail to honor its commitments[63]. As suggested by Das and Teng [63], the relational risk is affected by the goodwill trust, i.e. the expectation that some others in our social relationship have moral obligation and responsibility to demonstrate a special concern for others interest above their own [63]. Control is defined by the combination of three different components. Behavioral control focuses on the process which turns appropriate behavior into desirable output [63]. Output control is whether or not the alliances achieve the objectives of the partner firms, given satisfactory cooperation [63]. Social control aims at reducing the discrepancies in goal preferences of organizational members through the establishment of common culture and values [63].



Element	Link to co-opetition elements
Goodwill trust	Players
Performance expectancy	Added values
Behavioral control	Rules
Social control	Rules
Output control	Rules
Relational risk	Tactics
Dynamic transaction costs	Cost
Monitoring - collaborative use of IOS	Resources

Figure 5.2: Elements of risk management and compliance in co-opetition

To enforce such control firms can use an inter-organizational information system. There are two roles for an inter-organizational information system: monitoring use as a supporting activity for social control and collaborative use as a supporting element for goodwill trust [84]. This monitoring activity makes the Inter-Organizational System (IOS) a high maintenance system, i.e. a critical resource whose maintenance cost needs to be managed over time. According to the technology adoption model (TAM), the purpose of the IS design is to increase user's behavioral intention to use the system, which positively influence the use the system to increase the performance of the alliance. The use of the system deserves an additional consideration due to the share of data among co-opeting agents. On the one hand, collaborative use increases the data share and lowers the cost of retaliation if one partner decides to quit the alliance, which Hart and Moore [105] define as shading cost. On the other hand, monitoring use increases the chances of quick retaliation if one company tries to disrespect its duties, leading to the agency problem with signalling described by Spence [227]. From TAM, we derive two determinants positively affecting behavioural intention: performance expectancy and effort expectancy. Performance expectancy is the degree to which an individual believes that using the system will help him or her to attain gains in job performance [244], which we identify as the alliance performance; the effort expectancy is defined as the degree of ease associated with the use of the system[244], which we define as the alliance effort expectancy. Finally, TAM asserts that the monitoring effort negatively affects the expected performance, which requires a trade-off between too much and too little monitoring. Dynamic transaction costs in our model refer to the monitoring and collaborative uses. A previously mentioned, we refer to [139] to claim that both uses of the system increase the dynamic transaction cost, which comprises the cost of persuading, negotiating, coordinating with, and teaching co-opeting companies. Such cost increases the required effort, which lowers the performance and the intention to use the system.

Hence, the third-party enterprise might decide to externalize part of the required activities. Under the basic assumption that risk, control and trust are correlated, figure 5.3 describes how two companies can increase their mutual trust by lowering the risk of cheating and by proving compliance. Each arrow has a name and a sign. A positive sign + is used for direct correlation, whereas a negative sign - is used for an inverse correlation.

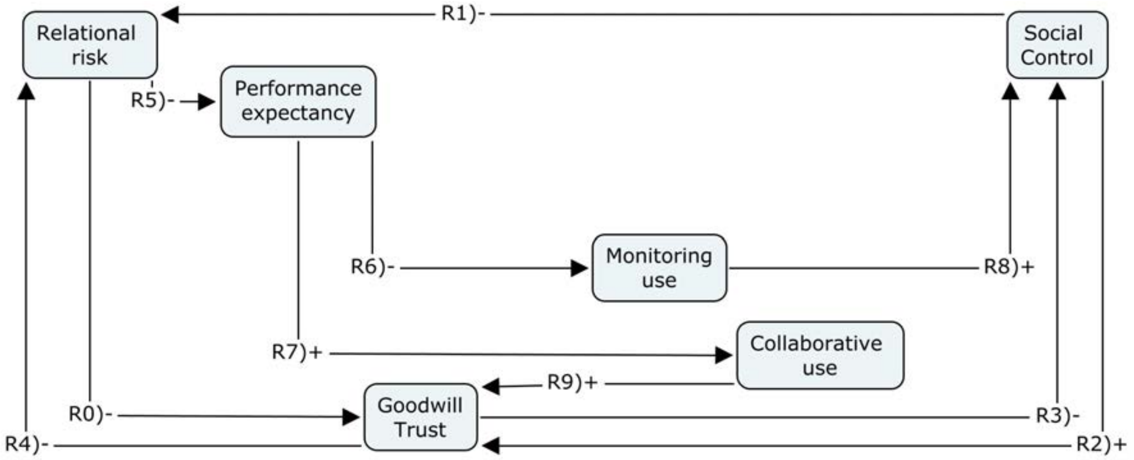


Figure 5.3: Relationships among elements of 5.2

As shown by relationship 0 (R0 in 5.3), the relational risk is affected by the goodwill trust. Social control reduces relational risk (R1) and increases goodwill trust (R2). Goodwill trust lowers the need for social control (R3) and the perceived relational risk (R4). The expected alliance performance has a mediating effect (R5) between relational risk and social control (R6) as well as between relational risk and goodwill trust (R7) [84]. There are two roles for an inter-organizational information system: monitoring use (R8) as a supporting activity for social control and collaborative use (R9) as a supporting element for goodwill trust.

5.2.3 Extending the existing literature

Co-opetition is a special kind of alliance that deserves additional considerations, which we present here under the shape of research sub-questions. The framework developed by Gallivan and Depledge [84] applies to the issues surrounding the use of an IOS between firms in an alliance. However, it does not make any distinction between the cases when the firms are competitors (i.e. have a co-opetitive relationship) or non-competitors (i.e. have a collaborative relationship). Taking into account that an alliance between non-competitors precipitates changes in the way that the use of IOS relates to the performance of the parties, we address this issue as a gap in the IOS literature. A third-party could make a profit by reducing transaction costs among co-opeting agents. The framework developed by Gallivan and Depledge [84] identifies two major uses for the IOS: monitoring and collaborative use. Based on the TCE, we claim that the companies can decide whether to internalize or externalize such functions to a third-party as presented in 5.4. Option A refers to the situation where the IOS is kept in-house by the alliance parties, as described by Golnam et al. [93]. In this case, no third party is involved, and it shall not be treated any further.

Option B occurs when the monitoring functions of the IOS is delegated to a third party. In such a case, the third party is mainly an audit company, which monitors the performance of the companies in the alliance. In such a form of alliance, the third-party is not in charge of conducting innovation. Therefore, it shall not be treated any further, since it falls outside the scope of this paper. Option C occurs when collaborative functions such as knowledge sharing between the parties in an alliance are coordinated through a third party.

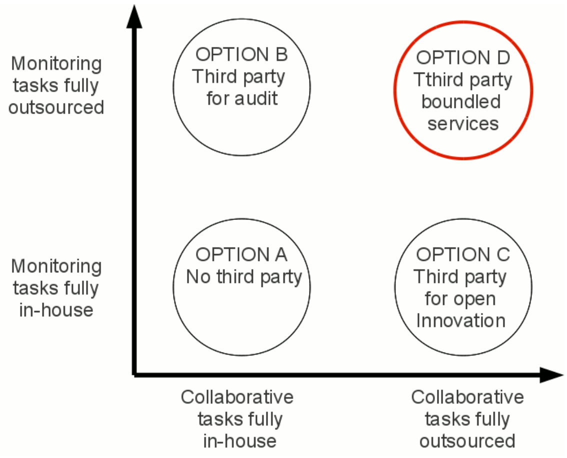

Monitoring tasks fully outsourced
OPTION B Third party for audit
OPTION D Tthird party boundled services
Monitoring tasks fully in-house
OPTION A No third party
OPTION C Third party for open Innovation
Collaborative tasks fully in-house
Collaborative tasks fully outsourced

Figure 5.4: Externalisation of R&D and monitoring tasks to a third-party enterprise (Option D)

5.3 Methodology

This section briefly underlines the chosen methodology. It presents the fundamental issues of design research in information system and it introduces the business model ontology used to develop our model.

5.3.1 Design science methodology

The distinguishing attribute of theories for design and action is that they give explicit prescriptions on how to design and develop an artifact, whether it is a technological product or a managerial intervention [96]. Therefore we address our three research sub-questions in three steps. The first research sub-question seeks for an explanation of the dynamics of co-opetition. An information system design theory (ISDT) should define its purpose and scope, i.e. the boundaries of a theory, which in our case is the design of a third-party to coordinate co-opeting firms in open innovation. The second element of an ISDT is the representations of the entities of interest in the theory (i.e. constructs). In addition to that the principles of form and function define the structure, organization, and functioning of the design product or design method [96]. Although it is mostly forgotten in most design papers the justificatory knowledge provides an explanation of why an artifact is constructed as it is and why it works. Therefore in the following section we list the elements of our model and we list the causal effects among them, grounding our statements into existing theories.

The second research sub-question concerns the dynamics of such system. According to Gregor and Jones [96] considerations of artefact mutability describe how flexibility and adaptability may be enabled by feedback loops to refine design. Thus at the end of the following section we propose a loop to make the system economically sustainable. The third research sub-question call for practical advices to implement and test the proposed model. The principles of implementation concern the means by which the design is brought into being - a process involving agents and actions [96]. Instantiated artefacts are things in the physical world, while a theory is an abstract expression of ideas about the phenomena in the physical world [96]. To define the evaluation strategy of testable propositions, a 2x2 matrix (ex-ante VS ex-post, naturalistic Vs artificial) is proposed by Pries et al. [189]. Hence the fifth section illustrates with second hand data how a firm can implement and test our proposed model by means of the business model ontology, which is explained in the next paragraph. The second hand data comes from a business case [136].

5.3.2 Business model ontology to develop a business model pattern

According to Osterwalder et al. [176] a business model ontology (BMO) or canvas can be described by looking at a set of nine building blocks. These building blocks were derived from an in-depth literature review of a large number of previous conceptualizations of business models. In this depiction, the business model of a company is a simplified representation of its business logic viewed from a strategic standpoint (i.e. on top of business process modelling). As shown in figure 5.5 at the centre there is the value proposition, which describes which customer's problems are solved and why the offer is more valuable than similar products from competitors. The customers are analysed in the customer segment, which is separated into groups to help identify their needs, desires and ambitions. The distribution channel illustrates how the customer wants to be reached and by whom he is addressed. In addition, customer relationships specify what type of relationship the customer expects and how it is establish and maintained with him. To be able to deliverer the value proposition, the business must have resources that they transform through key activities into the final product or service. Most of the time, a business depends on an external partner network to provide better quality or a lower price on non-essential components. As any business model would not be complete without financial information, the last two building blocks focus on cost and revenue. The cost structure should be aligned to the core ideas of the business model, while the revenue streams should mirror the value that the customers are willing to pay and how they will perform the transaction. By using their business model canvas, Osterwalder and Pigneur [175] present a set of business model patterns. A business model pattern describes some components of a business model and their relationships as well as how they can be applied to similar situations. As with patterns in other fields, these recurrent solutions for similar problems allow the company to elicitate requirements and ideas for improvements. The following section describes our proposed pattern for third-party enterprises managing co-opeting companies that perform open innovation.

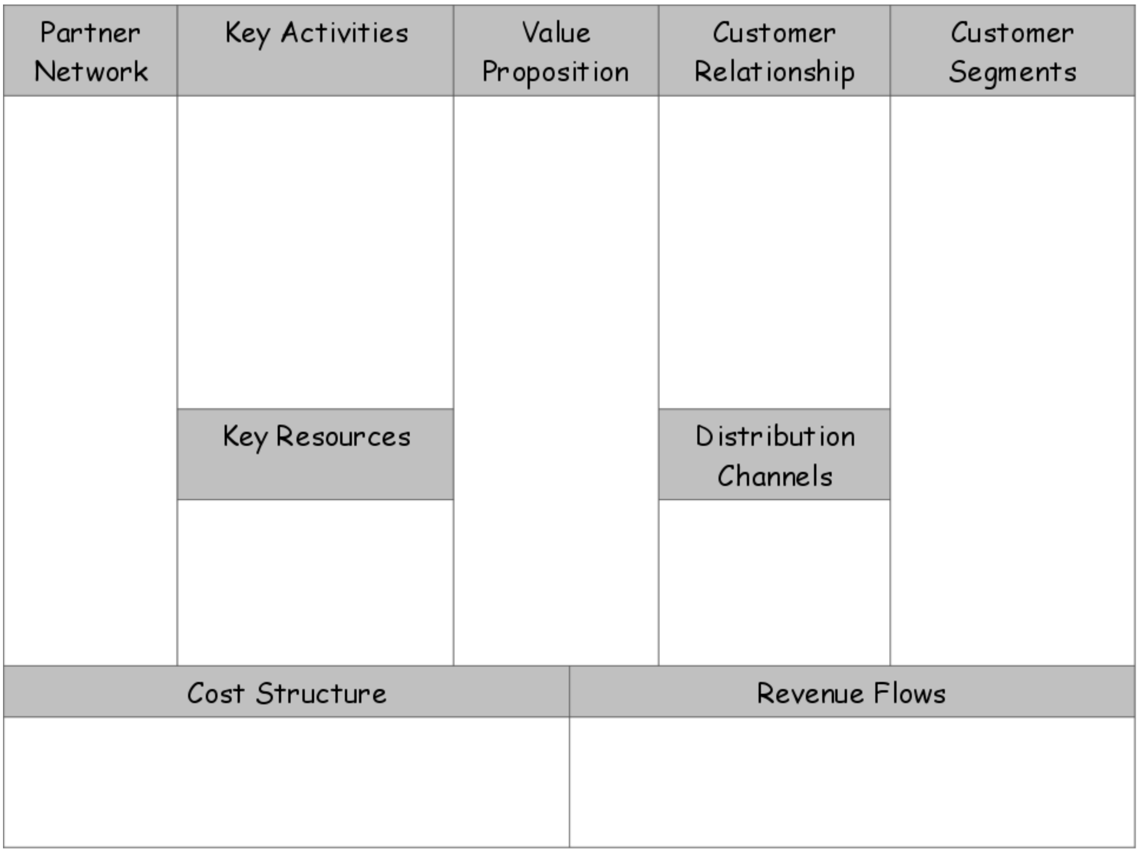


Figure 5.5: The Business Model Ontology

5.4 A business model pattern for co-opetition in open innovation

This section describes a conceptual model that extends the previous frameworks to give a consistent view of the dynamics of an alliance among co-opeting companies.

5.4.1 Three main loops derived from the theory

The system presented in this section has three main functions: monitoring competitors (figure 5.6), sharing data for cooperation (figure 5.7), and managing the dynamic transaction costs (figure 5.9). We describe in details each of the three figures, by starting with the set of relationships among constructs, which we derive from previous works, and by concluding with the new relationships among constructs, which we propose. As shown in figure 5.6 the system supports the creation of formal agreements regarding the innovation alliance by reducing ambiguity among co-opeting companies. Links R1, R5, R6 and R8 in figure 5.6 were derived from the existing literature concerning trust, risk and control. From TAM comes a new construct, i.e. the behavioral intention to use the system. The performance expectancy identified as the alliance performance positively affects the intention to use the system, which negatively impacts monitoring use (P1 in figure 5.6). Note how the links indicate that P1 has the overall same effect of R6. Therefore, our first set of propositions is the following:

Proposition 1: The performance expectancy has a mediating effect between the perceived relational risk and the behavioral intention to use the system.

Proposition 2: The behavioral intention to use the system has a mediating effect between the perceived relational risk and the monitoring use of the inter-organizational system.

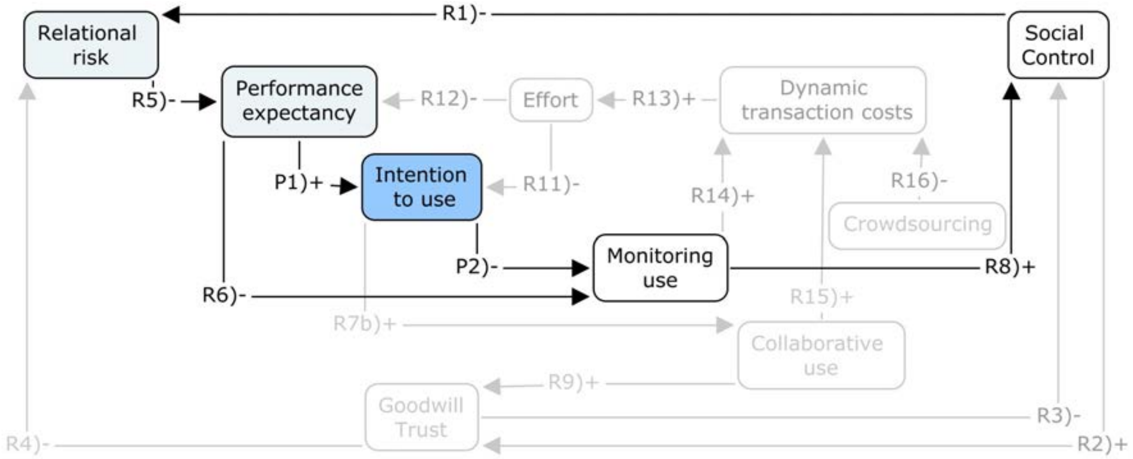


Figure 5.6: The monitoring use of the IOS to reduce risk among co-opeting agents

As shown in figure 5.7 the system supports the management of the innovation alliance among co-opeting companies by lowering their knowledge boundaries. Links R4, R5, R7 and R9 were derived from the existing literature concerning trust, risk and control. TAM adds the behavioural intention to use the system. The performance expectancy positively affects the intention to use the system, which positively impact the collaborative use (P3 in figure 5.7). Note how the links indicate that P3 has the overall same effect of R7. Therefore, the third proposition is the following:

Proposition 3: The collaborative use of the inter-organizational system has a mediating effect between the behavioral intention to use the system and the goodwill trust among co-opeting companies.

As previously shown for figure 5.7 links R1, R4, R5, R8 and R9 in figure 5.9 have been derived in the previous section from the existing literature concerning trust, risk and control. From TAM, come the behavioral intention to use the system and the construct regarding the expected effort. Links R10, R11 and R12 are derived from TAM and have been empirically proven many times in the past. Therefore, the focus here is on the role of the dynamic transaction costs of using the IOS. Such costs increase the expected effort of using the system (P4 in figure 5.9). The three links in P5 underline the influence of crowdsourcing to lower dynamic transaction costs and to indirectly increase performance expectancy. Therefore, our final propositions are the following:

Proposition 4: There is a direct correltation between the dynamic transaction costs of the alliance and the perceived effort required for using the inter-organizational system.

Proposition 5: The dynamic transaction costs of the alliance have a direct correlation with the monitoring use and the collaborative use of the inter-organizational system and an inverse correlation with the implementation of crowdsourcing.

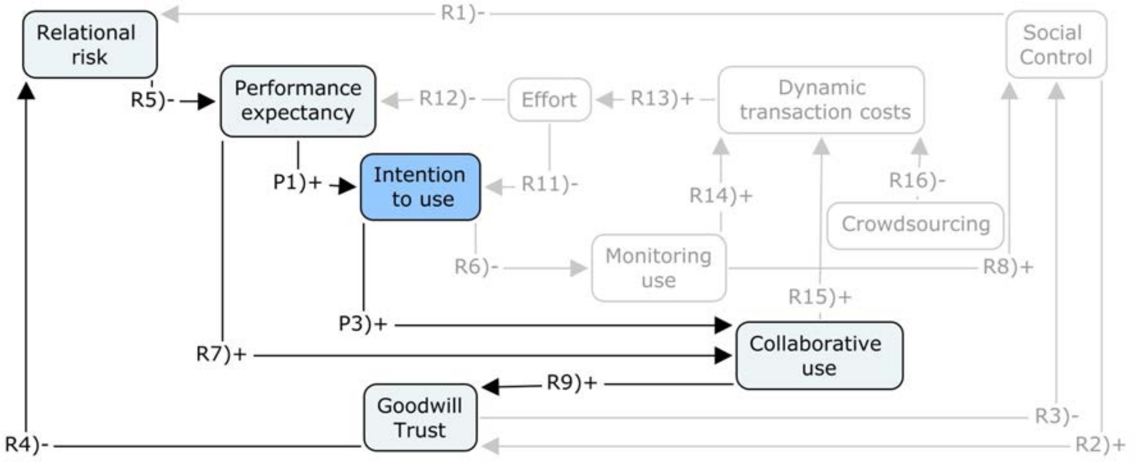


Figure 5.7: The collaborative use of the IOS to create value among co-opeting agents D and compliance.

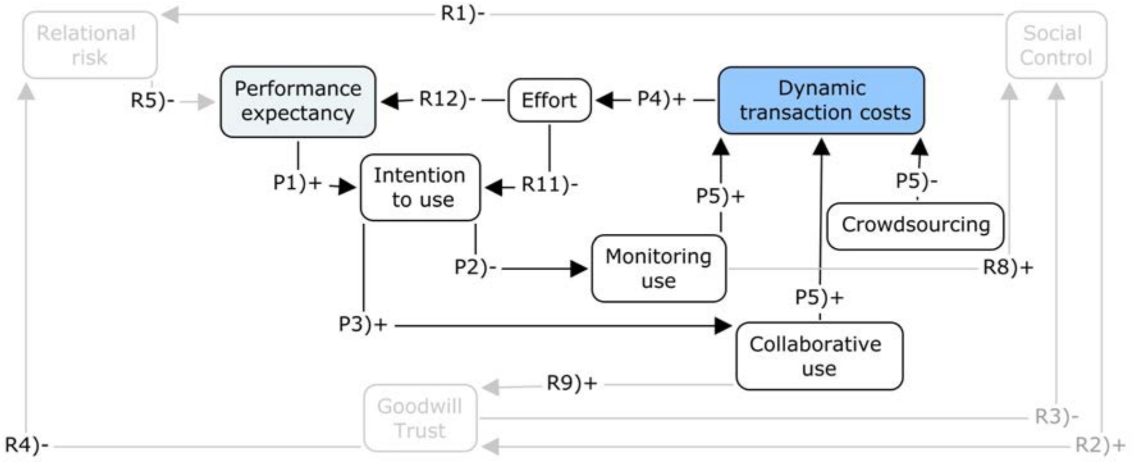


Figure 5.8: Crowdsourcing to lower dynamic cost of control

5.4.2 The overall model

We present now the overall picture that includes the three figures previously described. By merging the three loops previously defined, a new conceptual model arises and it extends the theoretical body of knowledge on which it relies. By combining theoretical frameworks of multiple domains, the model presented in figure 5.9 gives a more insightful view of a co-opeting alliance and is suitable to support policy, technical and business decisions.

5.5 From conceptual model to business model pattern

Pries-Heje et al. [189]proposes a testing methodology for IS design research. In our case, an initial evaluation of our proposition can be performed by collecting expert opinions regarding the positive impact of third-party enterprises on the alliance performance of

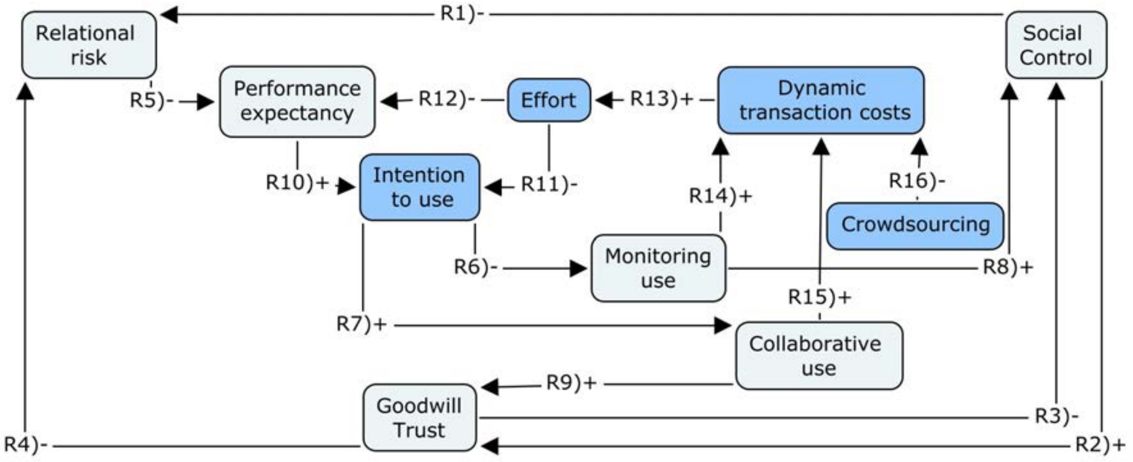
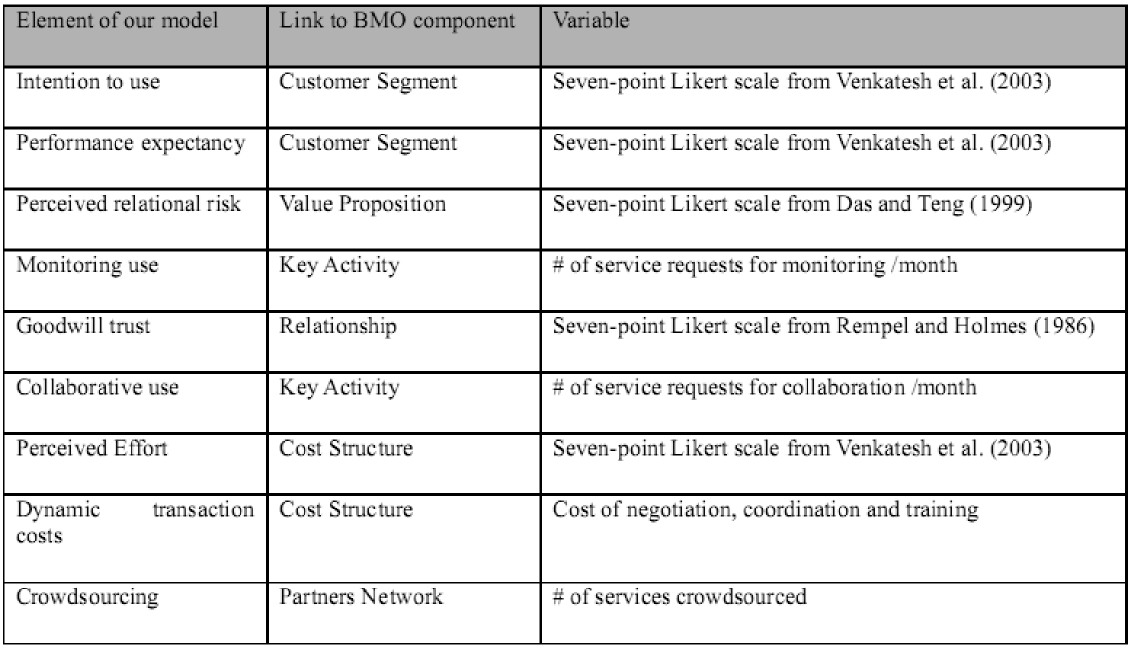


Figure 5.9: The new conceptual model for risk management among co-opeting agents

co-opeting companies. This sort of evaluation would be ex-ante, since the system would not be built yet, and artificial, because it would involve real users of a hypothetical system for real problems. As real users (referred here as problem experts) are more likely to think in business terms, the rest of the section illustrates how to convert our conceptual model into a set of business model components using business model ontology (BMO). The intention to use the system and the performance expectancy shown in 5.10 can be tested by a questionnaire for each type of user, identified as a customer segment, using the seven items defined by Venkatesh et al. [244]. We refer to Das and Teng [62] for the 14 questionnaire items to measure the perceived relational risk.

For the second proposition data from questionnaire is combined with an estimation of the monitoring frequency. To make such an estimate more reliable, we suggest using a scenario-based questionnaire as proposed by Barrett et al. [15].The test of the third proposition we suggest the approach proposed for the second proposition. To test goodwill trust, we refer to Rempel and Holmes[204]. For the perceived effort in the fourth proposition we suggest using the four items defined by Venkatesh et al. [244]. The dynamic transaction cost can be derived with the same technique used to estimate the number of service requests for collaboration and monitoring. The test proposed for proposition 5 includes the amount of crowdsourcing done to reduce the dynamic transaction costs and can be estimated collecting expert's opinion by means of scenario-based questionnaires.

Once the business model components are derived, the business model ontology (BMO) supports the implementation of the business model in a company. By managing and enforcing risk management rules at the strategic level this approach allows a company to obtain a consistent solution. Our solution comes as a double-sided business model [73] that bases its value proposition on the alignment of different customer segments that gain from the network effect of converging on the same platform. From the three loops, three possible users of the system (i.e. customer segments) are derived: legal agents drafting and implementing agreements for mutual control, business agents seeking new opportunities, and technical agents in charge of containing the IT costs (intended here as total cost of ownership and total cost of failure). Accordingly three value propositions are implemented:



Element of our model	Link to BMO component	Variable
Intention to use	Customer Segment	Seven-point Likert scale from Venkatesh et al. (2003)
Performance expectancy	Customer Segment	Seven-point Likert scale from Venkatesh et al. (2003)
Perceived relational risk	Value Proposition	Seven-point Likert scale from Das and Teng (1999)
Monitoring use	Key Activity	# of service requests for monitoring /month
Goodwill trust	Relationship	Seven-point Likert scale from Rempel and Holmes (1986)
Collaborative use	Key Activity	# of service requests for collaboration /month
Perceived Effort	Cost Structure	Seven-point Likert scale from Venkatesh et al. (2003)
Dynamic transaction costs	Cost Structure	Cost of negotiation, coordination and training
Crowdsourcing	Partners Network	# of services crowdsourced

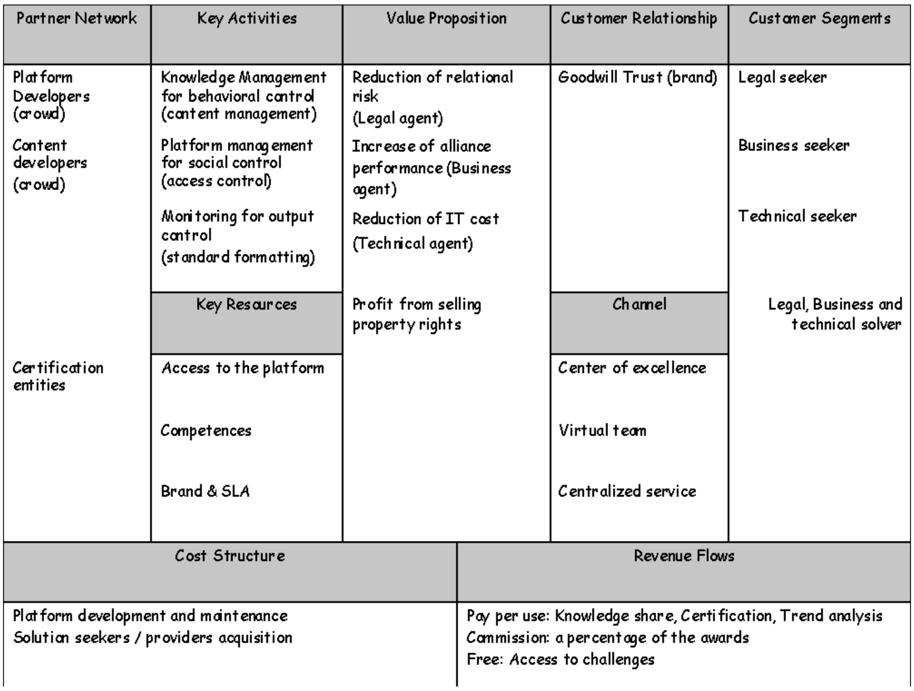
Figure 5.10: Operationalization of our theoretical model using the business model ontology (BMO)

relational risk reduction for the legal agent, increase in alliance performance for the business agent and lower dynamic transaction costs for the technical agent.

The distribution channel is a centre of excellence in charge of all steps and can take the three shapes presented by Cullen [59]: a best-practices sharing group, a virtual team or a centralized service. The relationship between the business units and the co-opeting agents relies on goodwill trust, which has been previously defined. The revenue flows include a fee to receive certification of positive behavioral control to be used by the legal agent as a proof of compliance. Another fee to access knowledge concerning best practices is previewed for the business agent, and a fee to access other parties' control results is offered for the technical agent. Social control is achieved by adding access control to the data regarding the outcome of the monitoring and content management activities. To reduce costs, the company externalizes the platform and content development to a crowd of partners and relies on certification entities to reinforce its brand, which is its key resource along with access to the platform. Hence, the cost structure reflects the special nature of a double-sided business model, whose major costs involve the platform development and management as well as the acquisition of solution seekers and providers to gain from network effects.

5.6 How to use the business model pattern: innocentive

This section applies our design to an existing and fairly well-known example of open innovation: Innocentive. Spun off in 2000 from Ely Lilly and its new business model



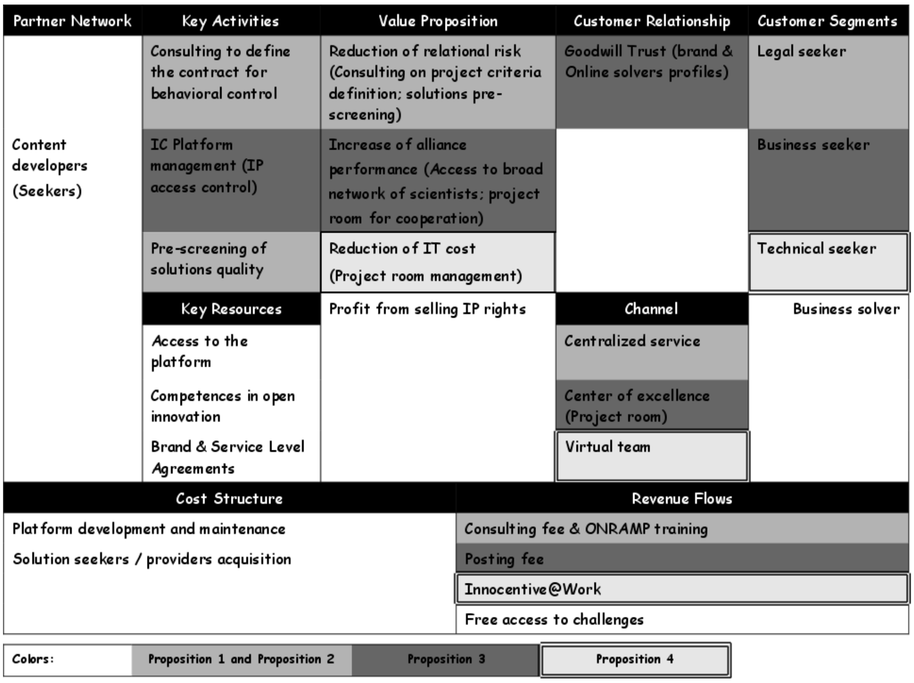
Partner Network	Key Activities	Value Proposition	Customer Relationship	Customer Segments
Platform Developers (crowd) Content developers (crowd)	Knowledge Management for behavioral control (content management) Platform management for social control (access control) Monitoring for output control (standard formatting)	Reduction of relational risk (Legal agent) Increase of alliance performance (Business agent) Reduction of IT cost (Technical agent)	Goodwill Trust (brand)	Legal seeker Business seeker Technical seeker
	Key Resources	Profit from selling property rights	Channel	Legal, Business and technical solver
Certification entities	Access to the platform Competences Brand & SLA		Center of excellence Virtual team Centralized service	

Cost Structure	Revenue Flows
Platform development and maintenance Solution seekers / providers acquisition	Pay per use: Knowledge share, Certification, Trend analysis Commission: a percentage of the awards Free: Access to challenges

Figure 5.11: Business model pattern for co-opeting companies performing open innovation

incubator e.Lilly, Innocentive is an independent intermediary that allows companies (known as seekers) to list their innovation challenges seeking for a solution. The rewards for the scientist solving the challenges (solvers) can reach up to $1,250,000. According to Osterwalder and Pigneur [175], the Innocentive value proposition lies in aggregating seekers and solvers by means of a platform that allows them to interact. In addition, Innocentive offers to seekers less risk, more reward [119], which can be seen as a reduction of relational risk for legal seekers. In this case, the co-opetitive business agents are seekers and solvers who belong to competing companies. For this purpose, Innocentive assures anonymity among solvers [136].The solvers obtain profit from their knowledge; hence, Innocentive allows each solver to sell the intellectual property right without disclosing the know-how that generates it. The legal agent of the seekers profits from the Innocentive consulting service to reduce the relational risk by drafting a good contract that describes the challenge to be solved [120].

Such contract has criteria that define both the quality required for the final outcome (output control) and the process required to achieve the outcome (behavioral control). The consulting service comes together with a training service called ONRAMP. Examples of challenges can be found on Innocentive website or on Lakhani [137]. For technical seekers, Innocentive offers IT cost reduction by hosting the open innovation platform. In this sense, collaborative software called Innocentive@work allows a company to leverage its employees' talent using a secure web portal. In this case propositions 1, 2, 3 and 4 would find a confirmation as shown in figure 5.12. Proposition 5 does not find confirmation, since Innocentive does not crowdsource the quality assessment of the solutions proposed. Lakhani [136] claims that Innocentive recognizes the need to facilitate exchange among solvers. A suggestion to modify the Innocentive website included limited voting (one for



Partner Network	Key Activities	Value Proposition	Customer Relationship	Customer Segments
Content developers (Seekers)	Consulting to define the contract for behavioral control	Reduction of relational risk (Consulting on project criteria definition; solutions pre-screening)	Goodwill Trust (brand & Online solvers profiles)	Legal seeker
	IC Platform management (IP access control)	Increase of alliance performance (Access to broad network of scientists; project room for cooperation)		Business seeker
	Pre-screening of solutions quality	Reduction of IT cost (Project room management)		Technical seeker
	Key Resources	Profit from selling IP rights	Channel	Business solver
	Access to the platform		Centralized service	
	Competences in open innovation		Center of excellence (Project room)	
	Brand & Service Level Agreements		Virtual team	

Cost Structure	Revenue Flows
Platform development and maintenance	Consulting fee & ONRAMP training
Solution seekers / providers acquisition	Posting fee
	Innocentive@Work
	Free access to challenges

Colors:	Proposition 1 and Proposition 2	Proposition 3	Proposition 4

Figure 5.12: Innocentive's business model representation gives evidences to support our propositions

each Solver) to facilitate screening of the solutions. This could be seen as a hint that Innocentive is pondering to crowdsource part of the monitoring effort, a strategic option already shown in our business model pattern.

5.7 Conclusions

Our work addresses the management of co-opeting agents performing open innovation. The previous literature has identified two dynamic loops that an alliance should support in order to be successful. Our work extends such a framework by combining control theories, transaction cost economics, resource-based view theory and game theory to obtain the business model of a third party in charge of risk management in multi-agent contexts of information system regulatory compliance, such as co-opetition in open innovation, in order to achieve sustainable profits. We conclude by answering our three research sub-questions, which we derived by assessing the existing literature on co-opetition and risk management:

How to coordinate the collaborative and monitoring uses of an inter-organisational system?

We suggest inter-organisational information system (IOS) designers to add features supporting collaborative uses to increase trust among co-opeting agents, whereas monitoring uses of an IOS increase control among co-opeting agents. Such features increase the co-opeting agents' behavioural intention to use the IOS.

How to crowdsource the coordination and monitoring uses of an inter-organisational system?

We call for a reduction of maintenance cost of an IOS by means of crowdsourcing under the control of a third party. Such reduction makes the system economically sustainable and this reduction in control effort increases the co-opeting agents' behavioural intention to use the IOS.

Which are the business model components of a third-party in charge of coordinating co-opeting firms?

We use the business model ontology to derive a business model from the elements of our conceptual model for risk management among co-opeting agents. Such business model is instantiated in section six using the Innocentive case as an illustratory example of how we intend to further test our guidelines.

If our conceptual model is not falsified by the empirical test we briefly sketched, then our contribution will be a framework to achieve compliance among untrusted partners by business model design. From a managerial point of view the contributions of this paper lay in its new ways to obtain a sustainable profit from aligning co-opeting agents involved in open innovation. From an academic point of view, by defining the IT managerial, methodological and technological capabilities and processes, we hope to raise interest of information systems researchers in this direction of investigation, since we believe that such issues fall into the nomological net defined by Benbasat and Zmud [19]. The theoretical limitations of our claims concern their scope, which focuses on requirements elicitation within an alliance, and its domain of application, which is more likely to work in heavily regulated business fields that rely mostly on intangible assets (e.g. chemistry). In addition to that such claims focus on the individual level of perceptions, leaving aside for the moment the group and the organizational level [140]. That is why, at the theoretical level, we envisage future implementation of our conceptual model using systemic enterprise architecture methodology [249] instead of the business model ontology to derive technical specifications of the information systems.

Chapter 6

The man behind the curtain. Exploring the role of IS strategic consultant

Abstract

Most organizations encounter business-IT alignment problems because they fail to properly understand how well an enterprise software pack- age aligns with or fits their needs. Strategic consultants make a profit by reducing such external manifestations of the differences between the organi- zation's needs and the system's capabilities. Therefore it appears relevant to understand how consultants behave. Our theoretical model shows how a consultancy can assess the way to extract and to generalize knowledge from its clients. The share of a consulting firm's global knowledge is compensated with new local knowledge obtained from the client. Hence we underline a way to assess the quality of that contribution and the mutual knowledge exchange.

6.1 Introduction

The development, implementation, operation, support, maintenance, and upgrade of enterprise systems (ES) have given rise to a multibillion dollar industry. Nonetheless organizations encounter difficulties in achieving an adequate return on investment since they fail to properly assess the ontological distance between software capabilities and their organizational needs[208].

Consultants are often used to reduce the differences between the organization's needs and the system's capabilities. Yet their strategic role in this domain has often been neglected by scholars [187, 232]. Over a period of more than twenty-six years, the Strategic Management Journal has given large attention to top management teams, and increasingly to middle managers, but has not published a single article on strategy consultants [254]. Strategic consultants are sometimes considered magic wizards with unknown power. But the title of this article recalls that even the wizard of Oz was just a man with a fancy machine behind a curtain. The purpose of this article is to study that fancy machine, and how it can be used to produce magic.

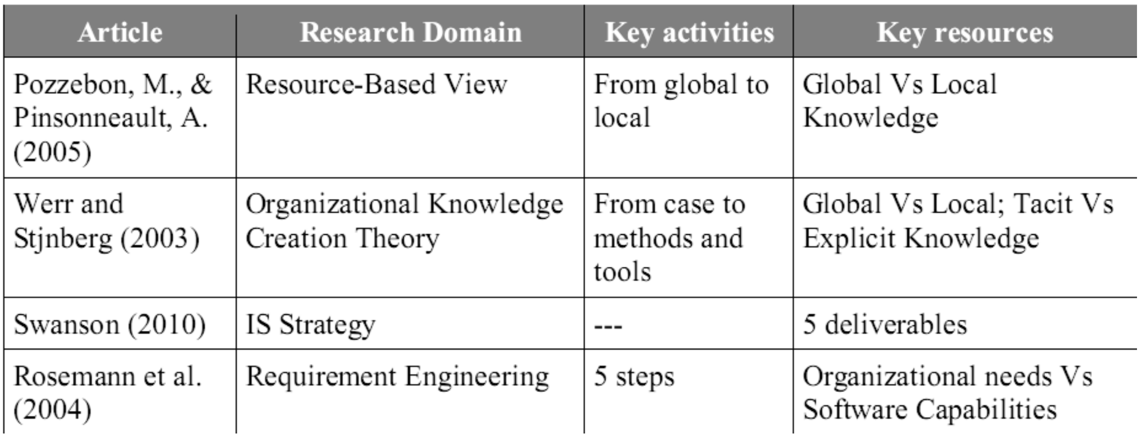
In the rest of the paper we take a look at IS Strategy, defined as 'the organizational perspective on the investment in, deployment, use, and management of information systems' [46]. The aim of this paper is to model IS strategy as a profession. In doing so we respond to the call by Whittington (2007), and we are interested in the risk reduction by minimization of the ontological distance between software capabilities and their organizational needs identified by Rosemann et al. [208]. The work of a consultant is an example of strategy as a profession and it is an archetype of a knowledge intensive firm. The most important assets (key resources) and actions (key activities) that a consultancy must use to make its business model work are worth investigating in detail. In this study we consider Small and Medium Enterprises (SME) offering IS strategic consulting. We ground our theory into practice by presenting the outcomes of a six-month internship in a strategic consulting firm which moved from its start-up status toward SME status by means of a shift toward business process management. Our research question is obtained accordingly:

RQ: How a small/medium strategic consultancy can positively use its expertise to gain a sustainable competitive advantage?

The main audience for this paper is composed of IS strategic consulting firms, which seek a sustainable advantage based on their core competences. We also hope to raise the interest of Chief Information Officers of companies which are clients of IS strategic consulting firms and which are interested in understanding how IS strategic consulting firms work. Finally we address IS strategy scholars interested in business-IT alignment, hoping to open a set of new directions to be explored. From a theoretical perspective, our model shows part of the elaboration of an IS strategy as profession and more precisely how to assess quality. From a practical perspective, our research helps both consultancies and CIOs to understand their work and improve the implementation of a configurable IT. The rest of the paper proceeds as follows. We start by reviewing the existing literature on IS strategic consultancies and identify the gaps to address through a set of research sub-questions. Then we introduce our theoretical model and suggest a set of testable propositions. For the sake of clarity, we address IS scholars and present the instantiation which we intend to use to test our proposition. Then we address to practitioners and describe how our theoretical model can be used in a business model. We conclude with a set of discussions and directions for further research.

6.2 Literature review

In this section, we present previous works on IS strategic consultancies and assess the gaps in the existing literature to refine our research question into a set of research sub-questions. According to Swanson [232] while they often appear as players, even major ones, in the IS field consultancies are rarely the focus of the research questions addressed (p.18). Since this topic is at the cross-road of different disciplines, we present four articles representing the contributions of four research domains.



Article	Research Domain	Key activities	Key resources
Pozzebon, M., & Pinsonneault, A. (2005)	Resource-Based View	From global to local	Global Vs Local Knowledge
Werr and Stjnberg (2003)	Organizational Knowledge Creation Theory	From case to methods and tools	Global Vs Local; Tacit Vs Explicit Knowledge
Swanson (2010)	IS Strategy	---	5 deliverables
Rosemann et al. (2004)	Requirement Engineering	5 steps	Organizational needs Vs Software Capabilities

Figure 6.1: The constructs of our model

According to Pozzebon and Pinsonneault [187] the role of a consultancy is to translate global knowledge, defined as generalizable features that may be divorced from particular settings and applied more widely (p.122) into local knowledge, i.e. practical knowledge that is highly specific to each particular firm and depends on the firm's employees (p.122). This approach grounded in the resource-based view [14] fails to detail the key activities required to pass from global to local and vice-versa. Werr and Stjnberg [252] focus on the importance of translating the experience of a consultant into a set of cases, which are local and explicit knowledge that contributes to the creation of global and explicit knowledge in the form of methods and tools. Such methods and tools are then converted into other cases and improved. This approach follows the stream of organizational knowledge creation theory summarized in Nonaka & Von Krogh [168], which focuses more on the dynamic creation of knowledge rather than the type of knowledge created. Swanson [232] extends the work of Werr and Stjnberg [252] by identifying five consultancy roles (Business strategy, IT research and analysis, Business process improvement, Systems integration and Business services). Each role is associated to a set of deliverables (in this paper we focus on the deliverables of the Business strategy role, which are a valuable input to this first stage of innovation, by creating a strategic framework for change). This approach, belonging to the field of IS strategy and innovation management, recognizes the role of the consultancy as an IT-broker but fails to explain in detail the process of requirement elicitation. Rosemann et al. (2004) do not address the role of consultancies, but identify two ontologies to be aligned: organizational needs and software capabilities, which we claim to correspond to local and global knowledge. This work, which comes from the literature in requirement engineering, drafts a five step process to align the two ontologies, but it is not concerned about how a consultancy could make a profit from this activity.

In conclusion, the existing research has not yet analyzed how to assess the quality of the global-local translation by a consultancy, how a consultancy can make a profit out of such translation, and what is the role of the customer in such translation. Hence, we derive the following research sub-questions:

- R-SQ1: How can the quality of the global-local knowledge translation process carried out by a IS strategic consultancy be increased.
- R-SQ2: How can an IS strategic consultancy gain a sustainable competitive advantage from a high-quality global-local knowledge translation.

– R-SQ3: What is the role of the customer in the global-local translation process?

From the literature review we also derive that there is no definitive formulation of the key activities and resources to be profitably used by a IS strategic consultancy, and that the existence of a discrepancy representing this issue can be explained in numerous ways. The choice of explanation determines the nature of the problem resolution. Thus the problem we address could be defined as wicked and best to be addressed using a design research methodology, as explained in the next section.

6.3 Methodology

In this section we briefly describe the methodology we used. Based on the relevant literatures, we create an artifact in the form of a model to express the relationship between local and global knowledge. We adopt a design science research methodology and refer to existing guidelines for design theories [96], which give explicit prescriptions on how to design and develop an artifact, whether it is a technological product or a managerial intervention (p. 312). Therefore we advance in three steps as illustrated in the figure below.

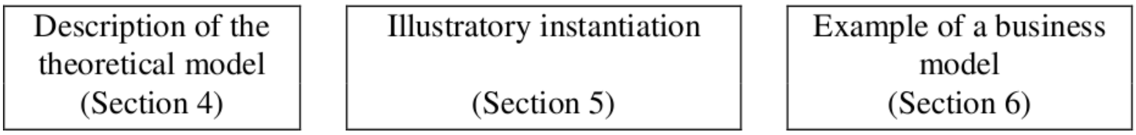
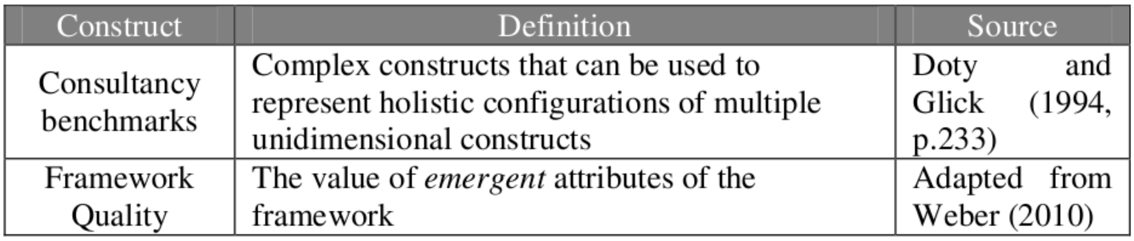

Description of the theoretical model (Section 4)
Illustratory instantiation (Section 5)
Example of a business model (Section 6)

Figure 6.2: Following sections

An information system design theory (ISDT) should define its purpose and scope, i.e. the boundaries of a theory. In our case, the theory relates to knowledge management to support customer retention. In this sense we introduce the representations of the entities of interest in the theory, i.e. constructs. The principles of form and function define the structure, organization, and functioning of the design product or design method. The justificatory knowledge provides an explanation as to why an artifact is constructed as it is and why it works. Accordingly in section 4 we introduce a model indicating how to assess the quality of the local-global knowledge translation. In doing so we ground our claims on existing theories of knowledge management, as well as principles of theory building. In section 5 we illustrate how to derive software requirements from our theoretical model by means of an example derived from the six-month internship in a strategic consultancy and we briefly illustrate our on-going evaluation strategy of testable propositions. In section 6 we present a possible use of our theoretical model by presenting a set of business model components for a consultancy.

6.4 The theoretical model

In this section we present a model that addresses our research question. We wish to extend the previous literature trying to explain how to best pass from local knowledge to

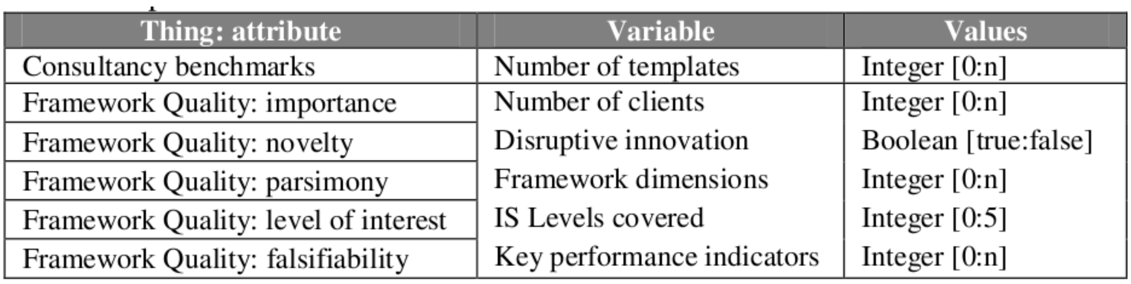


Construct	Definition	Source
Consultancy benchmarks	Complex constructs that can be used to represent holistic configurations of multiple unidimensional constructs	Doty and Glick (1994, p.233)
Framework Quality	The value of *emergent* attributes of the framework	Adapted from Weber (2010)

Figure 6.3: The constructs of our model

global knowledge. In order to do so, we introduce the notion of quality of the output in the translation process.

Our definition of consultancy benchmarks extends the definition of Werr and Stjnberg [252] for cases i.e. documents produced in projects, e.g. maps, process and proposals (p.889). Indeed we identify our benchmarks as ideal types of a typology and we measure them collecting the number of templates used by the consultancy. The benchmarks are collected within a framework, which in the words of Weber [247] to define a theory, is a particular kind of model that is intended to account for some subset of phenomena in the world (p.3). The concept of theory recalls Pozzebon and Pinsonneault's [187] idea of global knowledge. According to Weber [247] the quality of a theory can be evaluated in part and in whole. The quality of the whole framework can be assessed using five criteria: importance, novelty, parsimony, level, falsifiability. The importance of the framework can be measured by the number of clients using it. The novelty of the framework depends on the level of innovation requested by the customer and could have two values. Swanson [232] claims that customers use consultancies to be at the same level as their competitors, rather than to discover disruptive uses of a new technology. A framework is parsimonious when it achieves good levels of predictive and explanatory power in relation to its focal phenomena using a small number of constructs, associations, and boundary conditions [247]. The guidelines to create a typology-inspired framework allow for meso-levels of precision. i.e. a good balance between too much precision and too much abstraction. The level of the framework can be measured using the types of IS consulting[232]: business strategy, technology assessment, business process improvement, systems integration, business process support. The falsifiability can be associated to the number of key performance indicators used in the framework. The table for the operationalization of our constructs can now be derived.



Thing: attribute	Variable	Values
Consultancy benchmarks	Number of templates	Integer [0:n]
Framework Quality: importance	Number of clients	Integer [0:n]
Framework Quality: novelty	Disruptive innovation	Boolean [true:false]
Framework Quality: parsimony	Framework dimensions	Integer [0:n]
Framework Quality: level of interest	IS Levels covered	Integer [0:5]
Framework Quality: falsifiability	Key performance indicators	Integer [0:n]

Figure 6.4: Operationalization of constructs

Once the constructs are operationalized we state our null hypothesis, which concerns a non-linear relationship between the quality of the framework and the number of consultancy benchmarks. The role of an IT-broker in the IS strategic consultancy is to align two customer's organizational needs and software capabilities. Since those two ontologies are finite sets, the marginal contribution of a new best practice will eventually have to go to zero, since it adds no knowledge. H0: The positive relationship between number of benchmarks and quality of the consultancy framework is not linear.

One possible trend of such a non-linear function can be derived by considering the framework as a sort of theory. Weber [247] explains that as the number of constructs, associations, and boundary conditions in a theory increases, the theory might be better able to predict and explain the focal phenomena. As some point, however, users of the theory will deem it to be too complex. The goal is to achieve high levels of prediction and explanation with a small number of theoretical components (Ockham's Razor)(p.8). Accordingly one could expect the framework parsimony to follow an inverted quadratic function as illustrated in the figure below.

H1: The positive relationship between number of benchmarks and parsimony of the consultancy framework follows an inverted u-shaped function.

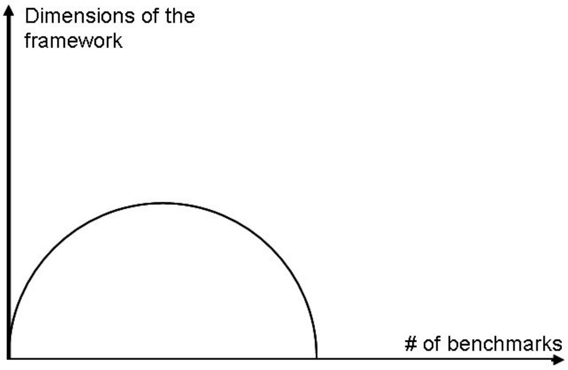


Figure 6.5: Example of an inverted U-shaped curve

Another trend is suggested by the literature on innovation, which leads us to believe that the relationship between number of benchmarks and framework quality should follow an S-shaped curve.

H2: The positive relationship between number of benchmarks and quality of the consultancy framework follows a logistic function.

Given this theoretical model in the following sections we wish to illustrate the guidelines to test its validity.

6.5 Illustratory instantiation

In this section we present how we intend to test our theoretical model using a repository for consultancy benchmarks. The figures used for illustratory purpose have been changed

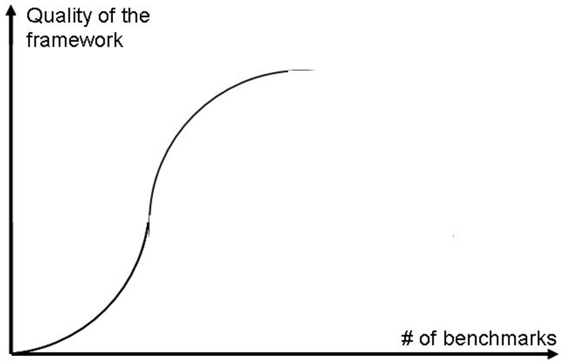


Figure 6.6: Example of a S-shaped curve

from the original images developed during the six-month internship at the consultancy to respect its confidentiality requirements.

Components: Goal oriented requirement engineering allows to express goals, tasks required to achieve the goals, and indicators to measure the task performance. A large amount of work already exists, the most cited being Van Lamsweerde [240]. Therefore we limit ourselves to claim that the first-order constructs of the consultancy framework can be represented using the goal oriented language (GRL) as goals and soft-goals, whereas the best-practices can be modelled as task, as shown in the figure below. To present the tasks in detail we have chosen to use the Use Case Maps (UCM) approach described in Buhr [37]. As illustrated in the figure below a process is composed of various tasks and sub-processes affected to various actors. The elements presented in this figure come from results of a six-month internship in a strategic consulting firm. According to figure 4 the Earning before Interest and Taxes is an indicator of the Profit increase. Cost reduction (measured by Yearly cost and Revenue increase (measured by Yearly revenues) have a positive effect on Profit increase. On the cost side the action Knowledge management has a positive effect on the element Best practices, which lowers the Yearly cost. On the revenue side the action Customer relationship management has a positive effect on the soft-goal Trusted relationship, which increases the yearly revenues. The main reason behind the choice of UCM is the possibility to combine GRL and UCM by means of the Unified Requirements Notation (URN) described in Amyot [5].

Architecture: We use the Eclipse plug-in called jUCMNav to implement our repository. For the moment we limit ourselves to the supporting processes of the strategic consultancy. Use case map (UCM) allows representing the 73 supporting processes in a consistent way, whereas the goal requirement language (GRL) is used to express the goals and soft-goals of the consultancy.

System mutability: The goals in GRL and the tasks in UCM are connected in URN. Once a new task is introduced it has to be linked to a goal to assess its contribution. In the same way, once a new goal is added it has to be linked to the existing set of tasks to assess its feasibility. This phase of the implementation has not been completed yet and will be used to verify our model.

Evaluation strategy: the evaluation of our instantiation is currently ongoing. During the six-month internship a set of iterations was set to formalize the processes of the consultancy.

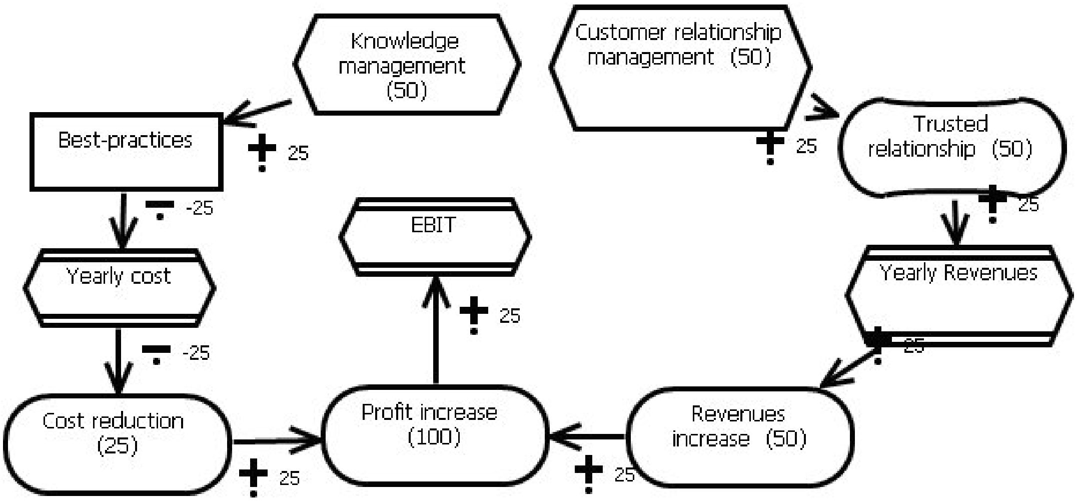


Figure 6.7: Example of GRL use to represent profit increase

At the end of each iteration an expert from the firm and researchers gathered to assess the quality of the work-in-progress. The first prototype for the processes was created using Visio to respect the existing software approach of the consultancy. Visio's prototype usability was tested through a survey. The second prototype using URN was created in the lab, leaving only the task-goal linking process left to be done by the consultancy. We expect that once we link goals to processes (considered here as benchmarks for consultants) the amount of soft-goals (dimensions of the framework) will follow an inverted u-shape, whereas the KPI, the number of soft-goals and the number of clients using the framework will increase following an S-shape.

6.6 Implementation of our model

In the previous section we illustrated how a consultancy can use its key resources to pass from client's local knowledge in its tacit form to global knowledge under the shape URN diagrams. We conclude now by suggesting how this could be profitable for the consultancy. In doing so we consider the consultancy as an example of strategy as a profession associated to a particular business model. The figure below shows that the business model ontology of Osterwalder and Pigneur [175] states that a company can offer a specific value proposition (VP) by combining key activities (KA), key resources (KR) and key partnership(KP). Such a value proposition is delivered through a channel (CH) to a customer segment (CS), with whom the company establishes a relationship (CR). The difference between the revenue flows (R$) and the cost structure (C$) is the profit for the company. In our case the main customer segment (CS) of the consulting firm is composed of the companies using its strategic advice. The value proposition (VP) offered to this customer falls into

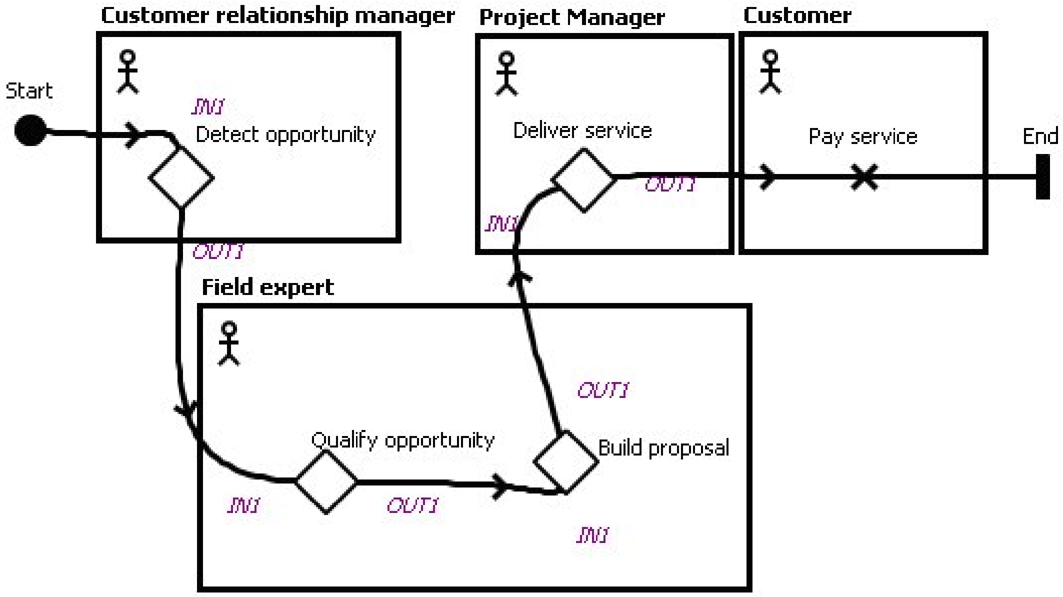
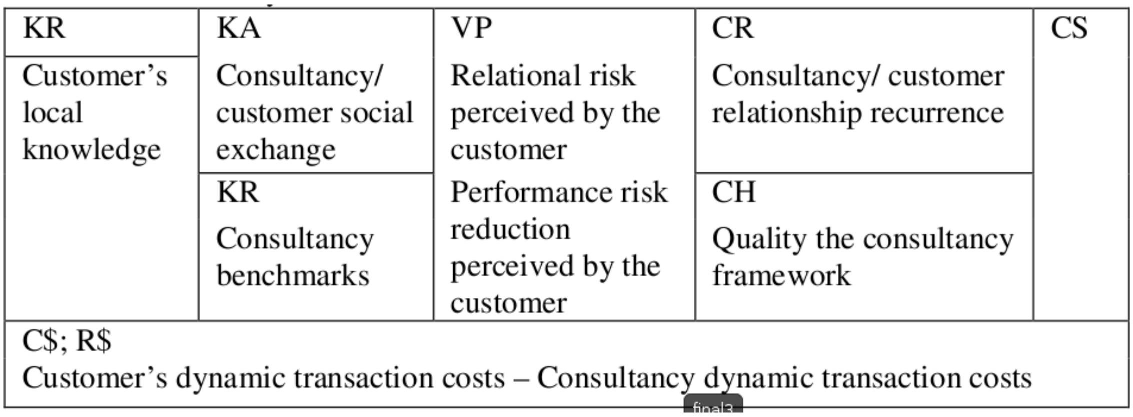


Figure 6.8: Example of use case map for contract management

five types of contributions to innovation with IT identified by Swatson (2010): Business strategy, Technology assessment, Business process improvement, Systems integration and Business support services. According to our research question we focus on the first type of contribution, and we are interested in the risk reduction by minimization of the ontological distance between organizational needs and software capabilities (Rosemann et al. 2004). The consulting provider delivers the channel (CH) services as a project. Each project has to respect a set of quality guidelines defined in accordance with the customer. One could consider the exchanges among the consulting firm and the customer as information economics. Therefore each project requires the consulting provider and the customer to manage a contract under asymmetry of information (Akerlof, 1970). Accordingly, the process is composed of four steps. At t=1 the consulting provider knows the quality of the service offered. At t=2 the customer offers a price in exchange for service quality, which can be accepted or refused by the consulting provider. At t=3 the consulting provider delivers the service. At t=4 the customer assesses the quality of the service against the agreement made at t=2. If the service quality complies with the agreement, the customer is satisfied and the consulting provider is paid. Regarding the customer relationship (CR) Rhenman (1973) acknowledges that there is in the consultant-client relationship an element of conflict.[. . .] Whether he realizes it or not, the consultant will become a pawn in the political game: his presence will always have some effect on the balance of power, sometimes perhaps a good deal. (pp. 160-171). Hence the customer agreement to pay might not be a good proxy for the quality of the service delivery. To address this issue we assume that the customer finds hidden costs after the payment, derived from a shading attitude of the consultant. But in this case the consulting provider is likely to not be hired again. Therefore we focus on project contracts that are managed among consulting firms and customers that have previously worked together, and we intend customer retention as a proxy of trusted relationship among a consultancy and its customers.

Among the key partnerships (KP) of the consulting firm are its customers since they are the source of local knowledge. On the one hand, in the role of information broker the consultancy delivers global knowledge and obtains local knowledge from each customer. On the other hand each customer can decide to hire one consultant. Therefore we identify these as co-opetition (Nalebluff and Brandenburger, 1997) relationships among the consultancy and its customers. In this type of this strategic alliance each strategic partners can decided to follow one of the four strategies suggested by Noteboom (2003). Since we limit ourselves to recurrent interactions among a consultancy and a firm, we focus on the so-called making attractive strategy, which is cooperative and fastening and which depends on mutual trust. The critical resource (KR) is the consultancy framework previously described. The critical activity (KA) is the global-local knowledge translation previously described. The revenue flow (R$) emerges from the satisfaction of the customer relative to the quality of the service provided and then the payment of the agreement. As previously mentioned in this paper, we focus on consultant contribution in Business strategy. The costs structure (C$) mainly emerges from the dynamic transaction cost and human resources. Dynamic transaction cost derives from the inability of the customer to internally create these capabilities (Langlois, 1992). Therefore consultants are more likely to contribute more to the processes by which firms imitate each other, than to those by which firms differentiate themselves (Swanson, 2010).



KR	KA	VP	CR	CS
Customer's local knowledge	Consultancy/ customer social exchange	Relational risk perceived by the customer	Consultancy/ customer relationship recurrence	
	KR Consultancy benchmarks	Performance risk reduction perceived by the customer	CH Quality the consultancy framework	
C$; R$ Customer's dynamic transaction costs – Consultancy dynamic transaction costs				

Figure 6.9: Consultancy as innovation broker

6.7 Discussions and conclusions

In this section we conclude addressing our research sub-questions:

R-SQ1: How is it possible to increase the quality of the global-local translation process which an IS strategic consultancy goes through? In table 3 of section 4 we present a set of five criteria to assess the quality of the consultancy framework and suggest the correlations among customer cases and consultancy framework quality. The idea of framework quality allows a consultancy to find the proper trade-off between the effort required to do the local-global translation and the creation of a competitive advantage.

R-SQ2: How an IS strategic consultancy can gain a sustainable competitive advantage from a high-quality global-local knowledge translation? Section 5 briefly introduces an instantiation of the framework using URN, illustrating how to convert our model into software specifications. Section 6 illustrates how to create a business model using of the consultancy framework.

R-SQ3: What is the role of the customer in the global-local translation process? Section 5 underlines how the customer is also the supplier of new cases. We identify a particular relationship between a consultancy and its customers. Both of them aim to access new global/local knowledge. In this co-opetition situation, customer trust is important in the consultancy and is the key for relationship success.

In conclusion we would like to recall our Wizard of Oz metaphor and the man behind the curtain. Trying to understand in which ways and under which conditions consultants contribute to their clients' learning and knowledge development (and vice versa), we have underlined one way to assess the quality of that contribution and the important role of mutual knowledge exchange to make it sustainable. At times, a consultant is like the Wizard of Oz, whose critical role is to lead the customer towards various quests to make him understand, at the end, that most of what he needs was already in his shoes.

Chapter 7

A set of control actions for a compliance support system used in a financial institution

Abstract

In this paper we address the elicitation of information system requirements for regulatory compliance, intended as a group decision between actors with conflicting goals. Extending the solutions proposed by previous authors in the field of multi-actor requirement engineering for multi-regulation compliance we claim that a set of patterns describing compliance-oriented services will lead to efficient, consistent and sustainable requirements for the information system. We shall illustrate the current state of the development of a typology, which we will present at the conceptual level, by means of its constructs, principles of form and functions. A fictive scenario inspired from a real case will allow us to discuss about the flexibility required to adapt the requirements to the regulations evolution. We shall conclude with some testable propositions to falsify our typology, together with highlights of the directions we intend to follow in order to obtain a handbook of patterns for regulatory compliance.

7.1 Introduction

So far most requirement engineering methods for Information System (IS) compliance have been proposed under the assumption that laws contain regulations that lead to frameworks, which are meant to support the definition of enterprise policies (for example see Tarantino[233]). From such enterprise policies, requirements are derived, IT solutions are implemented in the internal control system, which is audited periodically to assess its effectiveness.

In this article we question whether such process is linear, since in a multinational company time and space are two dimensions that impact the evolution of regulations in a complex

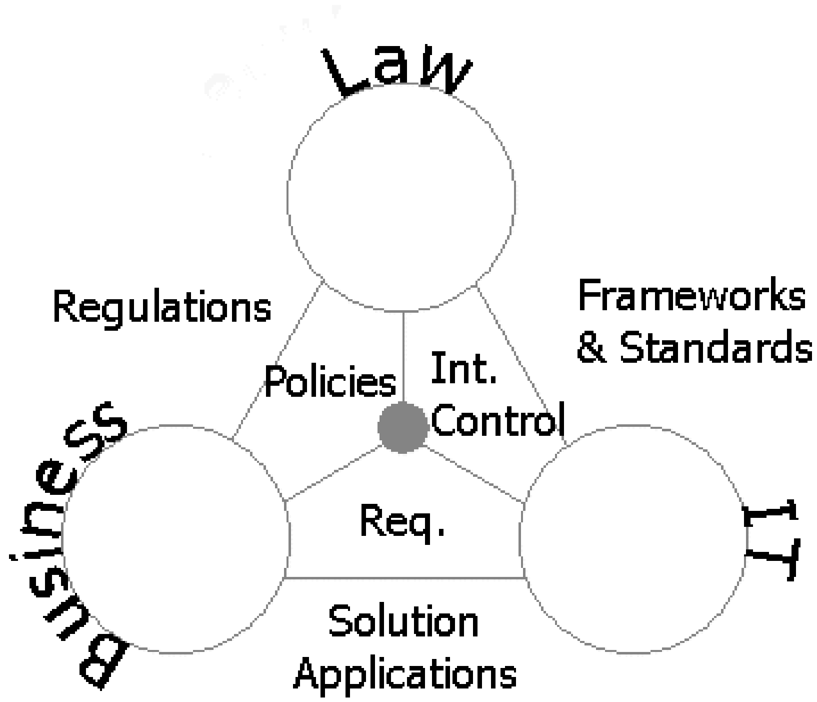


Figure 7.1: Law, Business and IT alignment

way. Previous works (e.g. the design of a multi-actors multi-regulations decision support system by Bonazzi and Pigneur[29]) considered the requirement engineering for regulatory compliance as an alignment exercise between the legal and the technical dimensions. We will extend that vision by adding the business dimension and identifying six types of stakeholder, namely three external to the company (a regulator that makes the laws, a group of practitioners that defines a framework of best practices, and an IT solution provider), and three within the company (a policy maker that define the enterprise policies, the compliance manager who assess the internal control system, and a IS solution architect that derives the IS requirements). The deliverable of each stakeholder is presented in figure 1, which represents the importance of a common ground for discussions between actors involved.

Our contention is that those six deliverables do not evolve in a cascade fashion. Moreover our experience leads us to claim that the six stakeholders involved have to be considered as having conflicting goals and yet a common interest in sharing their specific knowledge. The resulting group decision should deliver requirements that minimizes the long term costs for the multinational enterprise (efficient), that minimizes the changes among countries in which it operates (consistent), and that increases the return on investment of the IS solutions in place (sustainable). Hence our research question is:

how to support risk management in multi-actor contexts of information system regulatory compliance in order to achieve efficiency, consistency and sustainability?

In this article we derive our assessments from the resolution of concrete problems grounded into practice by means of four-month internship conducted in a major financial institution with headquarter in Switzerland, which has been solved by taking a design science epistemological stance and by performing an extensive review of the existing literature in governance, risk and compliance. We will present our preliminary results in developing a typology (as intended by Doty and Glick[70]) following the guidelines of Gregor and Jones[96] for a design theory. Hence section 2 starts describing the existing knowledge we will use to justify our claims. Then in section 3 we will move on describing the constructs of our underlying propositions. In section 4 we present a fictive case study inspired from a real scenario to illustrate how the control actions align the legal, business and technical dimensions. The following section will describe how we intend to support the elicitation of requirements in multi-actor, multi-regulations contexts. In section 6 we shall conduct a brief assessment of our proposed solution in terms of mutability. In the final section we shall propose testable propositions and further directions of investigation.

7.2 State of the art

To extend the requirement engineering process toward the multi-actors perspective means to acknowledge that there will be no interest in full data disclosure from actors in a co-opetition game where players cooperate and compete at the same time, as expressed by Beardsley et al.[16](the reader interested in co-opetition shall refer to Nalebuff and Brandenburger[163]). Indeed one can notice how the regulator wants to minimize the risk for the society, while the enterprise policy maker wants to maximize the profit for the company; at the same way the solution provider wants a solution that covers the greatest amount of cases, while the IS solution architect seeks for a solution that perfectly fits the existing architecture. In this sense the solution we seek should address first the problem of ambiguity (each actor does not understand the others, and does not have interest in being fully understood), to pass then to conflicting requirements. Moreover, since we take the point of view of the IS solution architect, we shall underline the concerns on evolution in terms of changes required in the system.

In this context and according to our research question we believe that to achieve efficiency most of the compliance process should be automatic. In this sense Giblin et al[91] proposed a solution to pass from enterprise policies to formal requirements. On year later Anton and Breaux [33] defined a way to automatically extract data from a regulation and starting from that point Siena et al.[220] have proposed an extension of i* identify the possible paths to pass from regulations to requirement, reinforcing the idea that a formal process is required to achieve intentional compliance (ex-ante) opposed to actual (on going) and strong (ex-post) compliance. Yet the authors do not explain how to choose the best path, even though Ghavanati et al. [89] assessed that, within the different compliance management approaches, a combination of tool-supported document-based (ex-post) and model-based (ex-ante) solution is the best. Thus the solution we propose shall balance the amount of formalism required and focus on decision support.

In what concerns consistency, one might recall the concept of holistic compliance that according to Volonino et al.[245, p. 217] stands in contrast to simply complying with the rules or silo compliance; i.e., efforts scattered throughout business silos and suggest that it is a matter of required actions for customization. Patterns (intended by Vaishnavi and

Keuchler [237, p.58]as a solution to problem in a recurring context, which is goal based rather than algorithmic) are usually used to enhance modular re-use and find a balance between standardization and customization. In this sense we mention the recent work of Compagna et al. [52] in identifying legal patterns modeled with i*, even though their proposed solution is said to be meant for a single actor.

Finally, the idea of sustainability recalls the concept beneath the idea of holistic compliance, i.e. to achieve the highest return on investment in compliance. In addition to that, we might recall that in a co-opetitive game, the only long term strategy is the one that assures the achievement of all stakeholders' goals. In this sense we refer to the recent work of Bagheri and Ghorbani[11] to combine stakeholders' viewpoints. Assuming that the viewpoints approach support the conflicts resolution, we shall focus our attention on how to reduce the ambiguity between stakeholders. In this sense O'Grady [172] has presented an extensive list of so-called compliance oriented architecture core services, even if the price of such extensiveness is a lack of precision and flexibility.

From what mentioned so far we identify a gap in the existing literature concerning the definition of a typology to align the legal, business and technical dimension, as shown in the figure 1. We also perceive that little interest has been given so far to the group decisions that lead to compliance, even though accountability is shared in case of an accident. Hence we propose to extend the work of Bonazzi and Pigneur[29] by defining a typology of so-called control actions, i.e. most common compliance challenges, presented here under the shape of patterns that a company can combine and re-use to lower costs and increase consistency, while maintaining a common language to increase the stakeholders understanding while expressing their viewpoints.

7.3 The proposed model

In this section we start by briefly recalling the constructs of the multi-actor multi-regulation dashboard we wish to extend, before introducing new ones. According to the authors a system to support to group decisions should allow the different types of stakeholders to express their viewpoints on the alignments concerning their domains of interest. Four constructs can be identified in the reference framework as illustrated in figure 2: the three previously mentioned (the business units, the regulations, the IT tools) and the one aimed conceived for the alignment(the control actions). Hence the policy manager will assign the different regulations to the business units, defining the why. The compliance manager will be in charge of assigning the different regulations to the set of control actions, i.e. linking the why to the what. At the same way the IS solution architect will assign the different control actions to the IS solutions tools, i.e. linking the what to the how.

In the rest of the paper we shall focus on the control actions, and in this sense we identify two core constructs, i.e. the action to perform (the taxonomy of actions shown in figure 3) and the direct object of the action (whose taxonomy is shown in figure 4). On the one hand such choice allows the creation of new control actions as combination of verb and direct objects. On the other hand it addresses the discrepancy of granularity between different regulations. Indeed while a regulation of a law might request to assure the effectiveness of the internal control system, another one coming from another law might

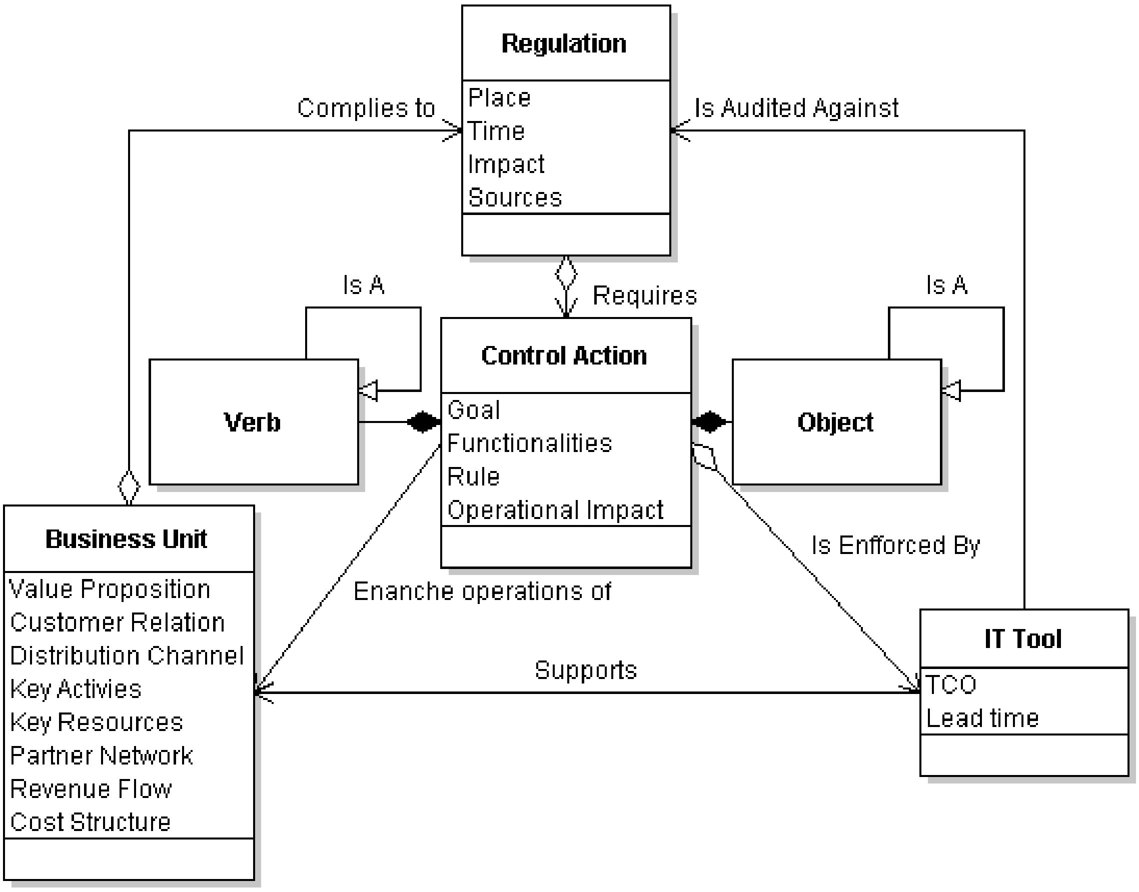


Figure 7.2: Constructs of our typology

specify that financial transactions have to be retained, even if it is implied in the first regulation. We obtained the two hierarchies getting inspiration from the COSO Enterprise Risk Management and the CobiT frameworks, and we adapted them to the context of the enterprise.

A short comment goes to the so-called functionalities in the verb taxonomy (they are not written in capital letters): those features do not exclude each other and possess an integer value above zero, as shown in the following section. The are the result of issues we encountered while enforcing some regulation, i.e. technical choices which were mostly not mentioned in the law but that could have consequences in case of legal case.

7.4 Expository instantiation: a fictive scenario

We have tested our typology by adopting them to model regulations coming from 17 laws impacting the IT. At the end we obtained ten control actions, one of which will be presented using a fictive scenario inspired from a real situation we experienced, i.e. using real terms but without entering into the technical details of a proposed solution, in order to help the reader feeling a glance of the challenge we faced. Hence we will describe the case

- MANAGE RISK
  - PREVENTING
    - PROTECT
      - ACCESS CONTROL
      - LOGIC SECURITY
        - Encryption
        - Data Loss Prevention
  - PROACTIVE
    - STORE
      - On Site
      - Worm
      - Retention Time
    - IDENTIFY
      - Digital Signature
    - MONITOR
      - ANTI MONEY LAUNDERING
      - RIGHT MANAGEMENT
  - REACTIVE
    - REPORT
      - Response Time

Figure 7.3: An extract of the Verb taxonomy

of a financial multinational company already complying with SEC 17a-4. For simplicity we will start assuming that a company has only one business unit that complies with this regulation. The characteristics of the regulations are shown in table 2. One can notice how the dimensions of time and space are represented. We are not going to treat here forecasting techniques required to estimate the impact of the lack of compliance to the regulation and we will assume that it has been calculated to $4.5 million. The references regarding the law and its reinterpretations should be included to allow all actors to have a precise and shared understanding of the topic.

REGULATION	SEC 17a-4
DESCRIPTION	Retention of traders' communications
PLACE	U.S.A. (Finance)
TIME	1934
IMPACT	$5M(fee)*0.9(probability)
ACTIONS	Store Communication [WORM=yes][OnSite=yes][Time=3]
SOURCES	http://www.law.uc.edu/CCL/34Act/index.html
	(R2003) http://www.sec.gov/rules/interp/34-47806.htm

Table 7.1: Example of a Regulation Form

Table 2 refers to a control action called "Store Communication", which is presented in table 3, and which is similar to the "Archive/Backup" service of O'Grady[172]. Such action is composed of the verb "STORE", which belongs to the proactive approaches according to figure 3 and the object "COMMUNICATION", which is composed of financial, mail, chat and SMS data, as shown in figure 4. Two possible functionalities are included, which concerns the application of the action: the data that is stored can be under the shape of Write-Once Read-Many (WORM), it could be stored on-site (which implies the data storing process cannot be outsourced or centralized between different business units in different

- REPORT
  - FINANCIAL RESULTS
  - ACTIVITIES
    - EMPLOYEES ACTIVITIES
    - CUSTOMER ACTIVITES
    - SUPPLIER ACTIVITES
  - TRANSACTIONS
    - COMMUNICATION
      - MAIL
      - CHAT
      - SMS
    - FINANCIAL
  - INTERNAL CONTROL
    - POLICIES
    - PROCEDURES
    - SOFTWARE
      - SOFTWARE LIST
      - SOFTWARE WEAKENESS

Figure 7.4: An extract of the Object taxonomy

countries) and it is usually retained for 5 years. The rule refers to the conflict-resolution strategy the company associated to this control action: if two control action of this type are present in the system (the first one requires data to be stored for 3 yrs, while the second one for 5 yrs), the one with higher values will be chosen. This is an example of a strategy which privileges risk-avoidance over cost-savings. The operational impact refers to the value added to the company by the implementation of this action and the value presented comes from Murphy's [162] estimation of cost to find required data in a legal litigation.

ACTION	Store Communication
DESCRIPTION	Communication are stored for further analysis
FUNCTIONALITIES	[WORM=no] [OnSite=no] [Time=3]
RULE	Maximize
OPERATIONAL IMPACT	[2000$/GB] (eDiscovery);
IT SOLUTION	Storing system

Table 7.2: Example of a Control Action Pattern

Table 3 refers to an IT solution, which is presented in table 4. Few data are required in our case and refers to the estimated Total Cost of Ownership (TCO) to implement the solution, together with the implementation time, which indicates in how much time it takes for the company to enforce the control action.

IT SOLUTION	Storing system
DESCRIPTION	Monitor different data channels and store indexed data
TCO	$ 3M (initial) + $50'000/yr
LEAD TIME	6 months

Table 7.3: Example of an IT Solution Form

7.5 Possible use of the artifact

In this section we suggest how the control actions should be used within the context proposed by Bonazzi and Pigneur[29]. Figure 5 presents the data flow, which starts from the collection of the four data types: two external (the laws and the control actions) and two internal (the business units and the IT applications). This data are presented to the three internal actors: the Policy maker (P), the Compliance Manager (C) and the Solution architect (S). Their subjective opinions regarding the link between data of different types (e.g.: the regulation SEC17a-4 is linked to the control action Store Communication, with a high degree of certitude) are expressed as suggested by Bagheri and Ghorbani[11] regarding Subjective Belief Base. The support system merges the new viewpoint and detects if there is an issue of ambiguity with previous viewpoints (e.g.: someone might think that the SEC17a-4 does not require the control action Store Communication). In this case the system underlines the ambiguity issue and informs the interested actors to let them discuss about it (the system does not take a decision, for which the actors would be accountable). If there is no ambiguity issue, the system solves eventual conflicts with previous rule using the control action strategy (e.g.: retention of e-mail of 5yrs instead of 3), and then presents the outputs under three shapes required for a correct governance: the presentation of the current situation, the required situation, and the gap between the two.

The information the gap contains, allows the managers to associate the decision to comply with a regulation to an option, which has a cost (the total cost of ownership of the IT solution) but it has a future profit (the operational advantages related to the introduction of a compliance service), together with the mitigation of a compliance risk (the cost of a penalty for not complying with a regulation).

As the reader might notice this solution also allows the three internal actors to achieve their goals. This way the IS solution architect will try to minimize the total cost of ownership (TCO) of the architecture while the solution provider will try to increase the number of control actions to increase the return on investment (ROI); on the same path the regulator will try to reduce the compliance risk and the total cost of failure (TCF) by assigning more regulations to each business unit. At the end we will have a set of business units complying with a large number of regulations, adopting a large number of hierarchically organized control actions, enforced by a small number of IT solutions.

Referring to our research question, the formalism used in pattern should allow performing the task automatically reducing the operational costs, their small number assures consistency and the large number of control actions implies a return on investment (mostly savings from quality increase of the other company services) that leads to sustainability. Still we have not fully explored that step yet.

7.6 Flexibility of the artifact against regulations evolution

We shall describe now two possible evolutions of the case presented in the previous section to assess the flexibility of our proposed artifact: a new interpretation of the regulation comes in, and a new regulation impacts the business unit.

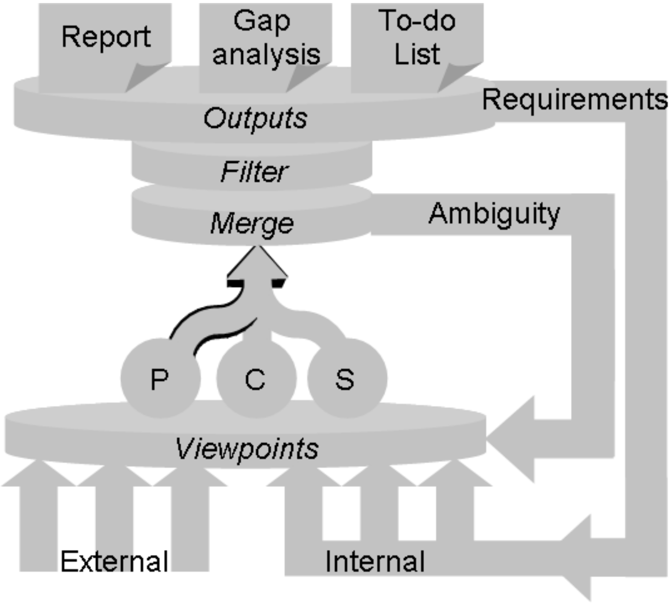


Figure 7.5: The data flow

In the first case we will suppose that a new interpretation of the SEC 17a-4 considers voice over IP (VOIP) data as being a communication to be stored. The Object hierarchy shall be extended by adding a VOIP element and specifying that it is a specialization of Communication. Accordingly, the storing system will have to fit the new requirements (in the real case previously described there was no additional cost for the chosen IT solution).

In the second case, we will suppose the existence of a new regulation that requires storing the e-mail for 5 years. On the one hand the company can choose to simply set the time parameter of the control action from 3 years to 5. Yet this solution would imply that all communications get stored for 5 years, which would mean a non-required cost increase. Thus the company might decide to expand the list of control action store e-mail which implements the same IT solution than store communication. As the reader might notice the two actions will conflict in what concerns the retain time of the e-mails, but since the conflict resolution strategy is maximize, the e-mail will be stored for 5 years, while the rest for only 3 years.

7.7 Discussions and Conclusions

We would like to conclude this article recalling the assessment of the compliance demands on IT for Sarbanes-Oxley according to Volonino et al. [245]: they are like those of Y2K—recurring four times a year. Our contention is that the challenge regarding multi-actors and evolving multi-regulations will become more and more stringent, and not only for multinational companies (as shown by the recent survey conducted over 700 Small and Medium Enterprises (SME) in Switzerland by Ernst and Young [36]).

As previously mentioned our research to address this challenge is still in progress, but we could list a set of testable propositions to falsify our typology:

P1: The control actions presented are more usable than the patterns proposed in previous works P2: The use of our control actions will lead to the elicitation of efficient, consistent and sustainable requirements. P3:A formal representation of the control actions will work well only in companies with a significant compliance process maturity level.

Referring to the first proposition the dashboard proposed in Bonazzi and Pigneur[29] allows compliance projects to not occur in isolation and to leverage existing specific acts and resources and assets, but does not enter in details concerning the components of each data set to be shared between stakeholders. Such components should be in a number greater enough to allow each actor to take informed decisions, without being too large to become a costly management misinformation system [1]. Hence a testable proposition would be to assess if the three internal actors involved find this solution for requirements elicitation as complete and easy to use. Moreover it would be interesting to test its adoption rate against the performances obtained using the solution previously proposed by Compagna et al. [52]. In this sense we speculate that our solution should perform better in terms of knowledge required for the use (we mostly require drag-and-drop) and flexibility of adaptation to regulations evolution.

Referring to the second proposition the solution we drafted in this article has to be developed in practice. On our side we developed a small prototype using Java programming language and we modeled regulations coming from some 15 laws and impacting the Information System of the company we worked with. From our experience we noticed an increase in communication between actors within the company, which led to a reduction in the number of compliance projects and in an increase of average budget allocated to each compliance project. Those indicators lead us to believe that consistency (less compliance projects) was achieved, while efficiency was expected (high budgets are justified if the expected ROI is high too). Regarding sustainability we refer what mentioned in previous section regarding the amount of effort required to adapt the requirements to the evolution of regulations. Yet our observations expressed here are derived by abduction from the results of a single case. Thus our proposition should be tested in other enterprises concerning the effect on number of projects and average budget following the introduction of our solution.

A last consideration goes to a technical extension cited in the third proposition, i.e. the possibility to represent the verb and the object taxonomies, and the control actions accordingly, by means of a knowledge representation language like OWL, or by process models following the recommendations of the Object Management Group. In this sense our testable proposition refers to the applicability of such extensions in contexts where the compliance management process maturity level is managed and measurable.

In the end we believe that the contribution of this paper is twofold. At the theoretical level it presented two classifications and put the seeds to the patterns handbook we want to develop to complete our typology. At the practical level it recognized the importance of the alignment between legal, business and technical dimensions by mean of a common language. We considered the regulations as options, that yield future profits at an initial cost, and we have shown how managers can use our solution to do so. We hope with our words to have raised the interest of the community in the research field we are investigating and we will welcome all contributions and remarks in that direction.

Chapter 8

A dynamic privacy manager for compliance in pervasive computing

Abstract

In this paper we propose a decision support system, for privacy management of context-aware technologies, which requires the alignment of four dimensions: business, regulation, technology, and user behavior. We have developed a middleware model able to achieve compliance with privacy policies within a dynamic and context-aware risk management situation. We illustrate our model in more details by means of a small prototype that we developed and we present the current outcomes of its implementation to derive some pointers for the direction of future investigation.

8.1 Introduction

Technology awareness concerns the understanding of the technological options for privacy management that are offered in a particular moment in time to the user. The link between pervasive computing and user's privacy risk has been addressed by many researchers, mostly in the field of location privacy. In his literature review of computational location privacy Krumm [133] claims that "location data can be used to infer much about a person, even without a name attached to the data."(p. 4). Most applications focus on controlling access and use of user's data, or they propose security algorithms to protect/obfuscate the communication of data between two users. Krumm [133] lists a set of solutions for location computational privacy. For example "blurring" is a security algorithm, which ensures a certain degree of location privacy by using inaccurate or at least not so accurate location information, in order to obfuscate the communication of users. Another algorithm is "Access control", which ensures that the sensitive data is only accessed by authorized people, in order to protect user's information privacy. Middleware development has been adapting to evolving technology, and in this sense we mention a solution that deals with conflicting privacy policies [43] and another solution that uses an extended version of a privacy policy language that takes into consideration the time dimension (Hong et al., 2005). In this paper we present the design of software for decision support regarding privacy risk management for pervasive technologies, with a particular interest in context-aware applications, as described by Schilit et al. [213] and Chen and Kotz [47]. Thus we aim at increasing the user's acceptance of the privacy management system. The theoretical foundation can be found in the technology adoption model proposed by Davis [65], which assess that user's behavioral intention to adopt a system depends on the perception of usefulness and ease of use. Thus a context-aware privacy management system should protect the user's data and it should reduce the number of actions requested to the user.

8.1.1 Awareness of changes in the commerce environment

A stream of research called economics of security, which Anderson and Blakely's research belongs to, has contributed in adopting economic concepts like "game theory with incomplete information" and "behavioral economics" into IS risk management (e.g. [2]). Recognizing the importance of privacy management as a business process, and a business support process, the use of a context-awareness application casts privacy management into a business perspective with benefits and costs to either party in a process. This is especially relevant for communications operators as brokers, and for communication channels between content owners (individuals, businesses) and enterprise applications. Privacy risk management is a situation where actors with diverging goals have a temporary interest in cooperating and sharing information to increase mutual trust [179]. Nalebuff and Brandenburger[163] describe this situation of cooperation and competition by means of five elements, which is used here as a general framework to assess the state of the art in academic literatures.

1- Actors involved in the game: Location privacy can be modeled as a non-cooperative game among peers [81]. In this case the phone user and her peers are identified as two selfish actors while the attacker is a third actor, whose goal is to obtain information about the phone user. The phone user and the peers have an interest in cooperating only once they get close enough to each other and can change pseudonyms in order to confuse the attacker. Extending the work of Hong et al. [114] a fourth actor emerges, i.e. the service provider, for example a weather forecaster of the zone where the phone user is located, who wishes to establish a trusted relationship with his potential users (i.e. he does not want to be considered as an attacker). Yet few authors seem to have recognized the importance of the privacy system designer, even if his actions affect other actors and although his goals are not necessarily aligned with any of those previously mentioned. One might recall the statement by Palen and Dourish [179] that privacy is the result of a set of dynamically evolving regulations between actors as their goals and level of trust change. Thus the way the system is designed might constrain the flexibility required by other actors.

2- Added value of each actor: Palen and Dourish [179] clearly identify the need for the phone user and her peers of a trade-off between the advantages of being visible to the others and the risk of exposure to an attacker. In what concerns the attacker beside the evident trade-off between the risk of being caught and the advantages of stealing personal data, Anderson [7] notices how an attacker has fewer resources than the security professionals, but aims at finding only one unknown bug to get an immediate advantage. This issue impacts the privacy system designer too, since he might not be the one who pays for the consequences of the theft of private data. This lack of moral hazard could lead to a phenomenon known as "liability dumping". On what concerns the service provider, one could expect him to look for the greatest number of potential phone users to reach with the least effort, and this could also be a case where the quest for network externalities (i.e. the search for more users to attract even more users) might be to the detriment of the security of private data. Again there is the possibility that the service provider could decide to act as an infomediary, i.e. an information intermediary [102] that collects data from the phone users and the privacy system designer and dispatches aggregated data while employing best-practices for privacy management. Such data would be valuable both for the phone users and to the privacy system designer, and will reduce its value to the attacker.

3- Rules of the game: On the one hand most authors agree on claiming that regulations concerning privacy management for pervasive technologies are still vague and ambiguous. Citing Massey et al. [152] "specifying legally compliant requirements is challenging because legal texts are complex and ambiguous by nature" (p.119). This might be due to the hard task that aligning business, technological and legal expertise implies. On the other hand a good example of clear privacy policies that can be understood by humans and machine is the Privacy Preferences Platform as described by Reagle and Cranor [203] and extended by Hong et al. [114]. On the technological side, many security technological solutions have been proposed and with the increasing computational power of mobile devices the number of offers is expected to grow exponentially. Yet on the business and legal side it is not clear yet how much control should be imposed on the actors involved and how much dynamism should be allowed.

4- Tactics for the players: Still to the best of our knowledge no author has dealt with the need of an evolution of the privacy system in the phone of the user, as a response of new ways to sense the environment and to enforce privacy policies. Among the security algorithm proposed for privacy protection Freudiger et al. [81] have taken into account the problem of user's selfishness in their pseudonym change algorithm, but no attempt to combine different tactics and to select dynamically one that fits best a determined state of the environment has been done yet.

5- Scope of the game: Regarding the scope of the interaction between actors, two dimensions come up to our minds. The temporal dimension suggested by Hong et al. [114] implies that the privacy system needs to evolve. For the data to be retained, while most authors focused on techniques to retain as little data as possible for as little time as needed, a quick consideration on the possible need in the future of data retention for regulatory compliance underlines the need of a middleware to mediate among different requirements. A second dimension to be considered is the geographical analysis, i.e. the size of physical area to be assessed. For sake of simplicity we shall assume it to be a circle, whose radius is 50 meters for the GPS-enabled mobile device and 100 meters for a Wi-Fi enabled mobile device.

8.1.2 Awareness of changes in the regulatory environment

Regulatory awareness concerns the continuous assessment of laws and standards that apply to a determined environment. From the regulatory point of view laws on data privacy are present in different business sectors and in different countries, leading to a complex multitude of overlapping and sometimes conflicting regulations that change over time, as described by Ponemon [185]. This commonly leads to ambiguity and to address that situation a standard privacy policy language, i.e. P3P [203] has been recommended by the World Wide Web Consortium. Although P3P has been criticized for its difficulty of implementation a stream of research has grown around it. Therefore we cite the recent work of Manasdeep et al. [149], who propose a collaborative model for data privacy and its legal enforcement to support a relationship of confidence between the operating system and the user's data repository. Another approach would be to use the set of metrics derived from privacy regulations, which can be found in Herrmann [108].

8.1.3 Awareness of changes in social environment

From the social point of view there are two levels of analysis which can be investigated. One could consider users' behavior as an external contingency factor that affects the privacy of a specific user, e.g. different cultures and countries are said to behave differently on what concerns privacy (e.g. Japanese are more likely to share data than Swiss users). Yet at the personal level user awareness is also an internal factor. Researches in human computer interaction have underlined this issue (e.g. [13]), but little has been done to design a privacy risk management application which takes into consideration those behavioral studies that represent users as opportunistic and rationally bounded. Most papers on privacy management implicitly assume a rational decision model, with the following characteristics: 1- Sure-thing principle: This was first introduced by the statistician Leonard Jimmy Savage [212] and it states that a decision maker can rank all options in order of preference and choose the highest one in the ranking. 2- Independence of tastes and beliefs: this assumption was proposed by the economists Roy Radner and Jacob Marshak [197] and it states that the decision maker's tastes concerning the outcome of the different options are independent of the options itself, and that her beliefs about the likelihood about the different outcomes are independent of the corresponding outcomes itself. In other words the decision maker is going to assess the outcomes and the likelihood of each option without any bias. 3- Logical and adequate capacity for computing: from the first two assumptions a third implicit assumption can be derived, i.e. that the agent should be logical and have potentially unlimited capacity of formulation.

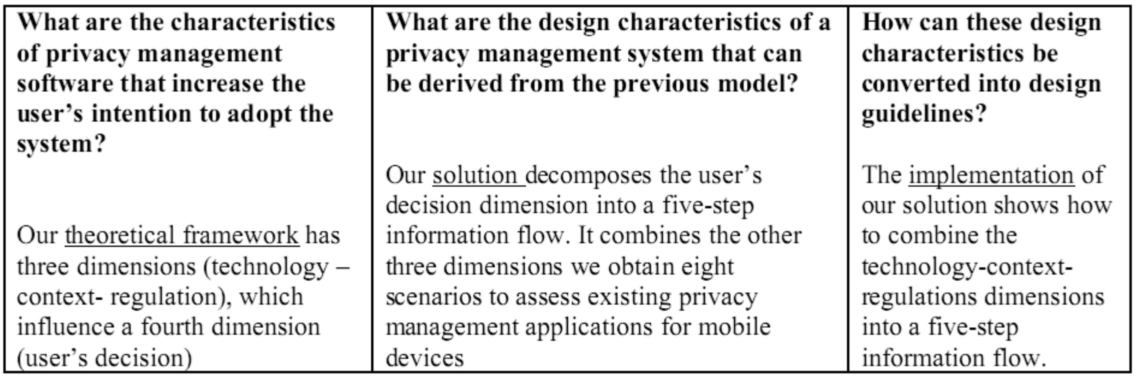
Simon [222] revised the rational decision model and relaxed the third assumption in his bounded rationality model. Indeed the logical approach to decision maker risk aversion does not imply risk neutrality. A rational user can be either risk neutral or risk averse. In the latter case the risk-averse user looks at the worst probable outcome (thereinafter indicated as "wpo") for each option and then chooses the option with the greatest "wpo" among the list. Therefore let us assume that someone has to make a bet on one of two options. Option A can let him win 100 euro or lose 50 euro, whereas option 2 lets him win 75 euro or lose 25 euro. If he wants to avoid risk he will rationally bet on the option B, since it has the greater wpo (-25 euro is greater than -50 euro). According to this model a decision maker starts creating options and ranks them sequentially. Once a satisfactory result is found the decision maker stops searching for other options. This is a dynamic decision rule strategy that drops the other options, even if they might perform better, because the cost of search is greater than the gain in performance. Radner [196] has proposed a "truly bounded rationality model" that acknowledges the cost involved in decision making (observation, computation, memory, and communication) and addresses the challenges in ordering the options (inconsistency, ambiguity, and vagueness of the options, unawareness of other options that might rise in the future) using a Bayesian model. But even such a model fails to determine the long-term outcomes of each option, making it hard to rank them properly. On what concerns security management, Straub and Welke [230] used the bounded rationality model to explain why managers take apparently irrational risk management decisions to minimize their perceived risk exposure. On what concerns perception Tversky and Kahneman [129] have shown that people tend to seek for opportunity and avoid risk in an unbalanced way. Therefore users might have the tendency to underestimate their exposures to privacy risks, which are hard to be perceived in the physical world. Therefore a privacy management application should support the user by decreasing the cost of decision making and by reducing the challenges in ordering the options. Otherwise the risk perceptions will be biased and the user is likely to be exposed involuntarily to risk. From the literature review it seems that the user dimension has received little attention from the information system community. Hence we investigate the implications of user awareness for privacy management system design in more detail. In doing so we assume that privacy risk management is a set of actions that the user expects his devices to perform dynamically in response to his perceived environment at a determined moment in time. Our research question arises accordingly: What are the design characteristics of a privacy management system for an opportunistic and rationally bounded user using a context-aware mobile device? In this study we follow a research design approach using the guidelines of Peffers et al. [182]. Thus the remainder of the paper is structured as follows: we start by briefly summarizing the methodology used in this study. Then we describe the design of our solution and how we came to develop it. After that we present a prototype, which we constructed according to our design and in conclusion we describe and illustrate a first evaluating session we performed with experts in the field.

8.2 Methodology

Based on the relevant literatures, we create an artifact in the form of a model [150] to express the relationship between user benefit and the amount of personal data disclosed[96]. Therefore we advance in three steps as illustrated in 8.1.

8.2.1 Theoretical framework

From the literature review we derive a set of constructs presented in figure 8.2. The first construct is technology awareness, which we define as the possibility for the mobile user to



What are the characteristics of privacy management software that increase the user's intention to adopt the system?	What are the design characteristics of a privacy management system that can be derived from the previous model?	How can these design characteristics be converted into design guidelines?
Our theoretical framework has three dimensions (technology – context- regulation), which influence a fourth dimension (user's decision)	Our solution decomposes the user's decision dimension into a five-step information flow. It combines the other three dimensions we obtain eight scenarios to assess existing privacy management applications for mobile devices	The implementation of our solution shows how to combine the technology-context-regulations dimensions into a five-step information flow.

Figure 8.1: From the theoretical model to the practical application of the design guidelines

receive updates about the security solutions available on the phone currently used. We suggest measuring this construct using the number of technological updates sent to the user's mobile device. The second constructs concerns context awareness, which we define as the possibility for the mobile user to receive updates about the privacy risk of the zone where she is currently located. We suggest measuring this construct using the number of sensor updates sent to the user's mobile device. The third construct is the regulatory awareness, which we define as the possibility for the mobile user to receive updates about the best combination "security solution"-"privacy risk" according to security frameworks and laws. We suggest measuring this construct using the number of rule updates sent to the user's mobile device. The fourth construct concerns the user's behavioral intention to adopt the system and it is based on the theory of reasoned action of Fishbein and Ajzen [76], whose explanatory power has been proved in the past by means of two metanalyses conducted by Sheppard et al. [218]. The technology adoption model of Davis [65] and its later extension called Unified Theory of Acceptance and Use of Technology of Venkatesh et al.[244] stated that a user's perceived usefulness increases the user's intention to use the system. User's awareness of the security technologies available supports the realization of user's identity protection. Therefore we claim that a user's behavioral intention to adopt the system follows the user's technological awareness in a linear way, as illustrated by 8.2.

Our first proposition can be expressed by the following formula:

(P1) User's behavioral intention to adopt the system = a1 + b1*Technological_Updates + n1

Where "a1" is constant that represents the fact that the user would adopt the system even if it does not offer any technological awareness. "a2" is a positive coefficient representing the relationship between the two constructs. "n1" is usually used in linear regression models to represent the difference between our estimated values and the actual values that are measured in reality. This difference is a consequence of variables that are missing in our equation. The technology adoption model of Davis [65] and its later extension called Unified Theory of Acceptance and Use of Technology of Venkatesh et al. [244] also assess that a user's perceived efficiency increases the user's intention to use the system. User's awareness of the surrounding environment allows him/her to clearly decide what

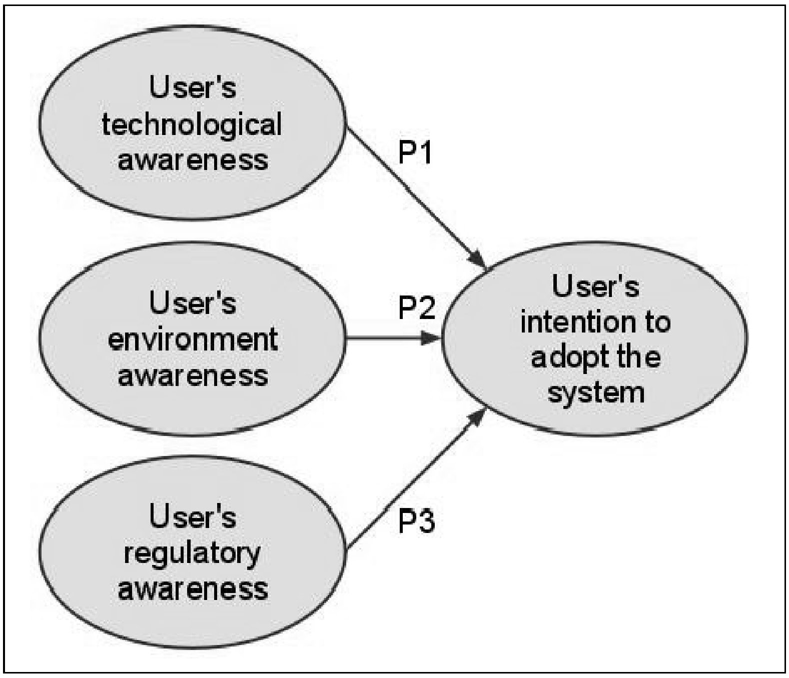

User's technological awareness
User's environment awareness
User's regulatory awareness
P1
P2
P3
User's intention to adopt the system

Figure 8.2: Our theoretical model

security technology to use and how to reduce waste of energy. We base this claim on the previous analysis of a user's bounded rationality and the consequent need of simplification. Therefore we claim that a user's behavioral intention to adopt the system follows the user's context awareness in a linear way. Our second proposition can be expressed by the following formula:

(P2) User's behavioral intention to adopt the system = a2 + b2*Environment_Updates + n2

Where "a2" is another constant, "b2" is a positive coefficient and "n2" takes into account the estimated noise effect created by the variables missing in our equation. The theory of trust, control and risk of Das and Teng [63], which has been applied to information systems by Gallivan and Depledge[84], describes how controls in place reduce the perceived risk and how that indirectly increases the user's trust in the system. The perceived risk can be decomposed into two parts: (1) the risk that someone steals the user's data, and (2) the risk that the system does not protect the data. The controls can be split into output controls (e.g. a log of all activities done on the mobile to identify intrusions), behavioral controls (e.g. the assessment of how a security algorithm works to protect the user data) or social controls (e.g. observing how surrounding people are behaving and are following the same norm). User's trust can be towards other people's good intentions or towards the system capacity to protect the user's data. According to this theory a user's awareness of the regulatory environment allows this person to understand the system's controls to reduce the environmental risk, and that increases the user's trust in the system and her intention to adopt it. We ground this claim on the previous analysis of user's co-opting relationship with the surrounding mobile users and the consequent need for mutual trust.

Therefore we claim that a user's behavioral intention to adopt the system follows the user's regulatory awareness in a linear way Our third proposition can be expressed by the following formula:

(P3) User's behavioral intention to adopt the system = a3 + b3*Regulatory_Updates + n3

Where "a3" is another constant, "b3" is a positive coefficient and "n3" takes into account the noise effect created by the variables missing in our equation.

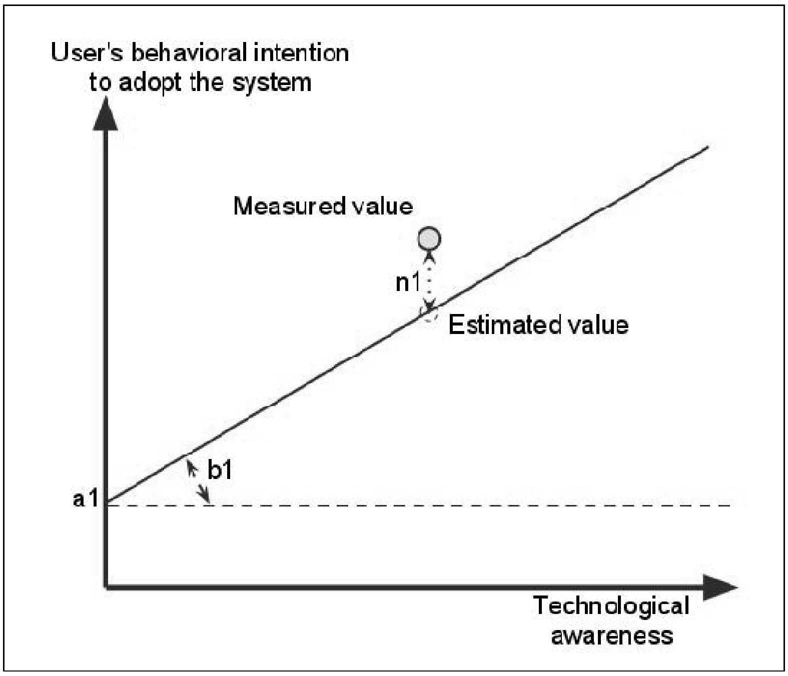


Figure 8.3: User's behavioral intention to adopt the system follows the user's technological awareness in a linear way

8.3 Solutions and reccomandations

8.3.1 Business implications of our model

Before passing to the technical implementations details of the framework, its business implications are worth to be investigated. Previous works regarding middleware for privacy management (Capra et al., 2003; Hong et al., 2005) have positioned their middleware on the server of the service provider. From the business perspective, this approach allows the service provider to obtain compliance in respect to privacy regulations. To give more data control ownership to users can lead to new value propositions, which in turn can defferentiate a firm from its competitor. A practical example of a firm that is currently gaining money from allowing the users to fine-tune their privacy preferences is the case Allow Ltd described by Angwin and Steel [8]. This London-based company negotiates with marketers on the behalf of users and obtains good deal for the users' data. The business opportunity rises from a proper context-regulation-technology model: in UK (context) the UK's Data Protection Act (regulation) allows user to remove their data from marketers' databases, by means of system (technology) that detects if the data was collected without user's permission. In addition that we suggest shifting the control of the privacy towards the mobile users, and that enables two additional value propositions: Greater performance for the privacy management system: in accordance to proposition 1 and 2 of our model the intention to adopt the system of the user is expected to be greater. Therefore one could expect the mobile user to be willing to pay more for this kind of software. Greater trust in the service provider: in accordance to proposition 3 of our model the trust in the system, and indirectly in the service provider is expected to be greater. Therefore one could expect the service provider to gain from the trusted relationship with the mobile user.

These types of business model considerations for mobile platforms have been already addressed in specific workshops, such as the business models for mobile platform (BMMP) workshop. In this sense Bonazzi et al. [23] have presented a set of business models that allows different key players in the mobile business sector to gain money from privacy management. But that article misses to explain in details how to technically implement each business model. Therefore we wish to extend their business models by adding a set of design guidelines to our framework.

8.3.2 Framework

8.4 shows the information flows among the four constructs of our framework illustrated in figure 2. We refer to the literature in decision making and use the process proposed by Straub and Welke [230] to list the five steps of a security risk plan implemented by our system. The first step is the recognition of security problem, defined by Straub and Welke [230] as "the identification and formulation of problems with respect to the risk of IS security breaches or computer disaster". In our case, the system gets awareness of the context by collecting data from its sensors (e.g. Wi-Fi, GPS, and Bluetooth). The second step is risk analysis (defined by [230]), "the analysis of the security risk inherent in these identified problem areas; threat identification and prioritization of risks". The system gathers the sensor data and assesses them using the updated roles database to assess the context data. The third step is the alternatives generation (defined by [230]), "the generation of solutions to meet organizational needs specified during risk analysis". A set of regulations might match the context. The profile that has the highest fit is automatically selected. The fourth step concerns the decisions (defined by Straub and Welke, 1998), "matching threats with appropriate solutions; selection and prioritization of security projects". For a given threat, the profile suggests a set of actions to be enforced. The fifth step is the implementation (defined by [230]), "realizing the plans by incorporating the solutions into the on-going security of the organization". The set of actions is enforced by the information infrastructure and the tuple time-sensor data-risk profile-actions enforced is recorded in a log by the system, for further compliance analyses.

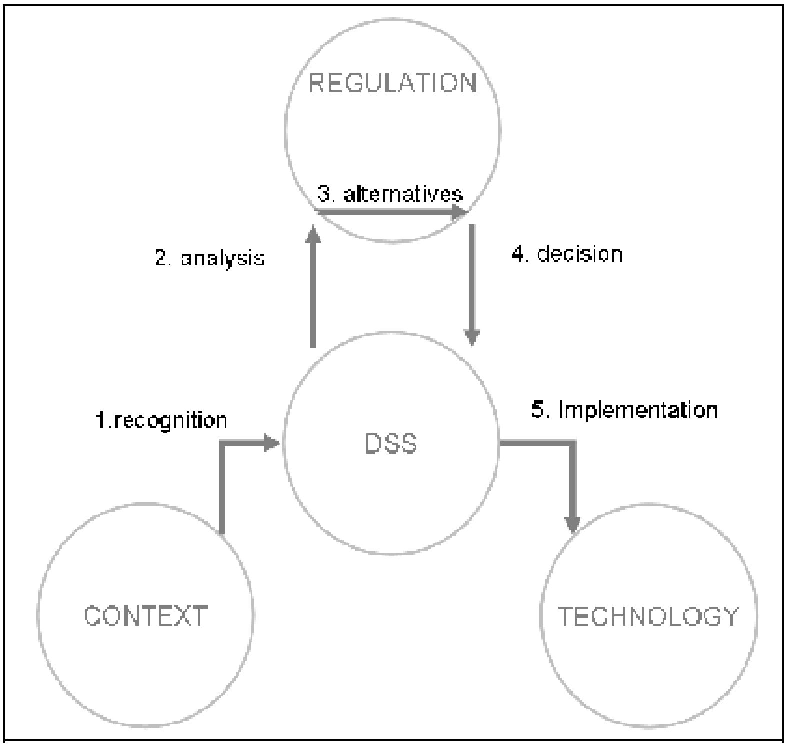
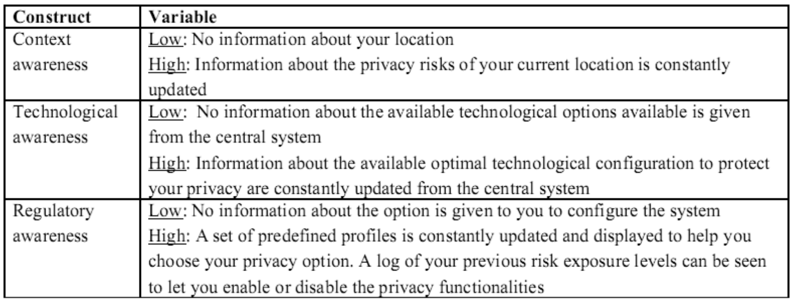


Figure 8.4: Information flow to support risk management decisions

8.3.3 A set of scenarios illustrating privacy risk management on the client-side

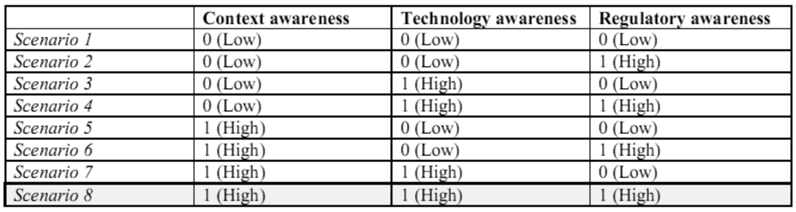
An information risk management approach in the context awareness lets the user achieve the best security level according to environmental threats she currently faces. The design solution envisaged makes use of state of the art technologies and constantly adapts to the environment to take a proactive stance against privacy risk. We operationalize the construct of our model, as illustrated in 8.5.



Construct	Variable
Context awareness	Low: No information about your location High: Information about the privacy risks of your current location is constantly updated
Technological awareness	Low: No information about the available technological options available is given from the central system High: Information about the available optimal technological configuration to protect your privacy are constantly updated from the central system
Regulatory awareness	Low: No information about the option is given to you to configure the system High: A set of predefined profiles is constantly updated and displayed to help you choose your privacy option. A log of your previous risk exposure levels can be seen to let you enable or disable the privacy functionalities

Figure 8.5: Operationalization of variables for the scenarios

We obtain 2 at the power of n different scenarios, where n is the number of constructs in our model, and 2 is the value that each construct can get (0=Low or 1=High). For the sake of clarity, we briefly describe each scenario, and we link it to existing applications for the Android OS. As the scenario number one does not concern any construct, we start with the second scenario. The second scenario describes the software that contains a set of profiles that have to be manually changed. Predefined rules are constantly updated from a central system. A log of user's previous risk exposure can be seen to let the user enable/ disable the privacy functionalities. For this scenario, two applications for Android already exist: "Privacy Guard" and "The eye". The third scenario describes the software that contains the information about the available optimal technological configuration to protect user's privacy which is constantly updated from the central system. For this scenario, we have found the following applications for Android: "Mobile Security$^{\text{TM}}$", "Lookout Mobile Security", "Antivirus Free", "Norton mobile" and "AVG antivirus Pro". The fourth scenario describes the software that combines the information of technological solution and regulation: information about the available optimal technological configuration to protect the user's privacy is constantly updated from the central system. A set of profiles has to be manually changed. Predefined rules are constantly updated from a central system. A log of the user's previous risk exposure can be seen to let you enable /disable the privacy functionalities. For this scenario, we have found the following application for Android: "MyAndroid protection 2.0". The fifth scenario describes the software that contains the information about the privacy risks of the user's current location and where this information is constantly being updated. For this scenario, we have found the following application for Android: "Glympse". The sixth scenario describes the software that combines the information of context and regulation. For this scenario, we have found the following applications for Android: "Locale", "Setting profiles full" and "Toggle settings". The seventh scenario describes the software that combines the information of context and technological solution. For this scenario, we have found no application for android but web services exists: "General crime", "Homicides" and "Victims". The last scenario includes all of the above three constructs. However, we could not find a corresponding application. Therefore in the rest of the paper we wish to explore the last scenario more in details. We start by illustrating two examples to distinguish the eighth scenario from the other seven, as illustrated by 8.6.



	Context awareness	Technology awareness	Regulatory awareness
Scenario 1	0 (Low)	0 (Low)	0 (Low)
Scenario 2	0 (Low)	0 (Low)	1 (High)
Scenario 3	0 (Low)	1 (High)	0 (Low)
Scenario 4	0 (Low)	1 (High)	1 (High)
Scenario 5	1 (High)	0 (Low)	0 (Low)
Scenario 6	1 (High)	0 (Low)	1 (High)
Scenario 7	1 (High)	1 (High)	0 (Low)
Scenario 8	1 (High)	1 (High)	1 (High)

Figure 8.6: Eight scenarios obtained by combining the three dimensions of our theoretical model

Example 1: sensors analysis for unknown environments Alice is a student at the University of Lausanne. She often uses her mobile phone to buy things online. In order to protect her privacy information from the privacy attacks in her surrounding environment, she installed the software "Privacy Manager" on her mobile phone. This software allows Alice to define and configure her privacy preferences, such as degrees of risk, types of potential attacks and corresponding solutions to protect her private information. After the configuration, the software automatically detects the connection information of mobile devices around her via sensor technologies on the phone. Once it identifies any unknown connections during her purchasing procedure, it responds by taking avoiding action to protect her privacy. For example, one day Alice buys a book when she is in the university. “Privacy Manager” detects that there are many unknown connections around her current position. “Privacy Manager” reports it and adopts two technological solutions (blurring and access control) to protect her online purchasing. After lunch, Alice goes for a walk near the Leman Lake. She wants to book a train ticket with her mobile phone. Again, “Privacy Manager” detects that there is 1 unknown connection. Here reporting a fake location (blurring) is not useful and it should be not implemented to save computational effort and battery energy. Thus “Privacy Manager” implements only “access control” to protect her information.

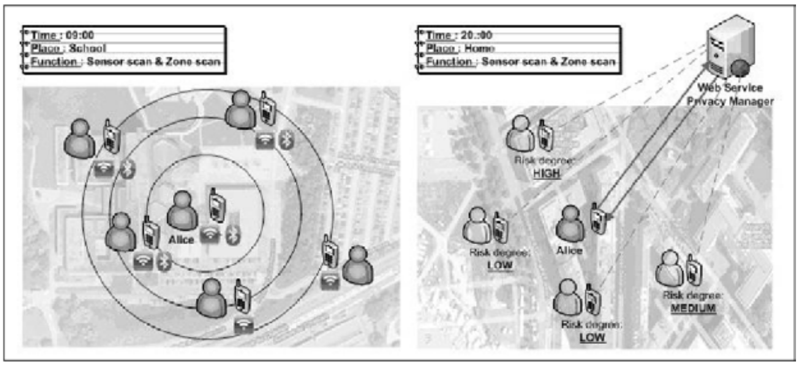


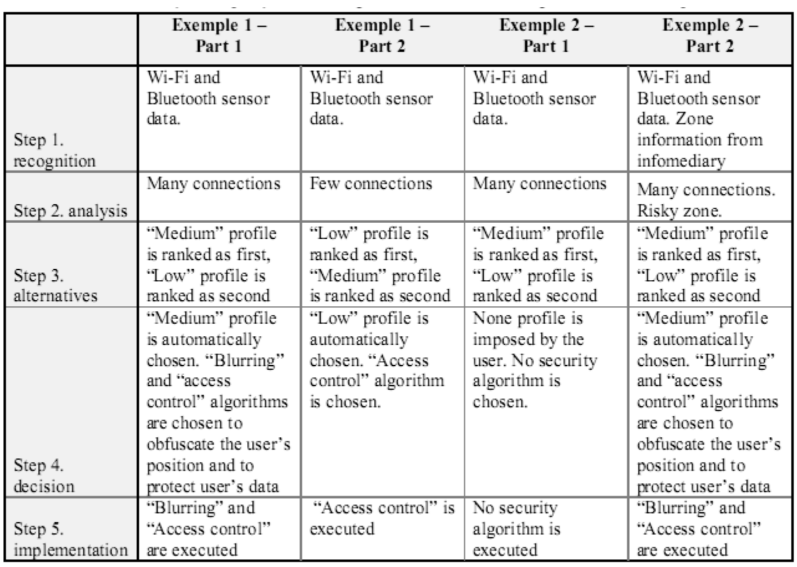
Figure 8.7: The first example (on the left side) and the second example (on the right side).

Example 2: aggregated historical data for known environments After class, Alice goes back home. “Privacy Manager” realizes it is a safe place according to Alice’s earlier set configuration and does not implement any protection actions. Now Alice is going to buy a CD online with her mobile phone. “Privacy Manager” allows her phone to connect to the web server and it gets historical data in this zone. This connection has been protected by the security firewall. By combining police database information and private users’ devices configuration details, the privacy manager web service can send information to Alice’s mobile device about the privacy risk of the zone where she is located. Therefore “Privacy Manager” suggests to Alice to increase her privacy protection level since many mobile users have claimed to have had their mobile phones stolen in that neighborhood. Finally, Alice takes Privacy manager’s suggestion and adjusts the risk profile to the “Medium” accordingly.

Table 3 links the two examples to the data flow for decision support presented in figure 4. As previously said the security algorithms have already been implemented with success in mobile applications. Therefore we shall present a prototype that illustrates how to enforce a set of security profile according to contextual privacy risk, which is assessed by means of data sensors collection and zone risk updates sent by a trusted third party.

8.3.4 Implementation

We implement a prototype of PRIVACY MANAGER according to the design guidelines discussed earlier. The overall goal in designing PRIVACY MANAGER is to examine the



	Exemple 1 – Part 1	Exemple 1 – Part 2	Exemple 2 – Part 1	Exemple 2 – Part 2
Step 1. recognition	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data. Zone information from infomediary
Step 2. analysis	Many connections	Few connections	Many connections	Many connections. Risky zone.
Step 3. alternatives	"Medium" profile is ranked as first, "Low" profile is ranked as second	"Low" profile is ranked as first, "Medium" profile is ranked as second	"Medium" profile is ranked as first, "Low" profile is ranked as second	"Medium" profile is ranked as first, "Low" profile is ranked as second
Step 4. decision	"Medium" profile is automatically chosen. "Blurring" and "access control" algorithms are chosen to obfuscate the user's position and to protect user's data	"Low" profile is automatically chosen. "Access control" algorithm is chosen.	None profile is imposed by the user. No security algorithm is chosen.	"Medium" profile is automatically chosen. "Blurring" and "access control" algorithms are chosen to obfuscate the user's position and to protect user's data
Step 5. implementation	"Blurring" and "Access control" are executed	"Access control" is executed	No security algorithm is executed	"Blurring" and "Access control" are executed

Figure 8.8: The five steps of risk management decision making in our two examples

feasibility of our approach and to understand the privacy issues possibly involved. We describe the prototype's system architecture, the frameworks used, as well as the graphical user Interface. In doing so, we give implementation details for Symbian platform (Nokia), even though a prototype for Android platform has been developed as well.

8.3.5 System architecture

Figure 6 shows the local privacy manager's interaction with the components of the privacy architecture and the web service. For the configuration of a user's located privacy policies, we use a XML file to store user's preferences on the phone. It allows the user to edit, create and delete their privacy policies at any time. Detecting the risk of environment is done by using the python socket architecture [80]; it provides the service of interactive communications between the different sensors of technologies. The local IT privacy solutions can be accessed directly via the information requests of users. The web service server receives and processes requests vis-a-vis the provider database, before requested data is sent back to the user via QtWeb Network Requests. The resultant information is finally transmitted by the web service to a user-friendly GUI using HTML.

8.3.6 Implementation details

The application PRIVACY MANAGER for Symbian platform is mostly written in C++, with the toolkit Nokia Qt, which is a cross-platform application and UI framework. It includes a cross-platform class library, integrated development tools and a cross-platform IDE. Using this toolkit, the web-enabled application can be written and deployed across embedded operating systems. The XML file stores all service provider information, including the risk criteria given by present data, the context of current situation, as well as the

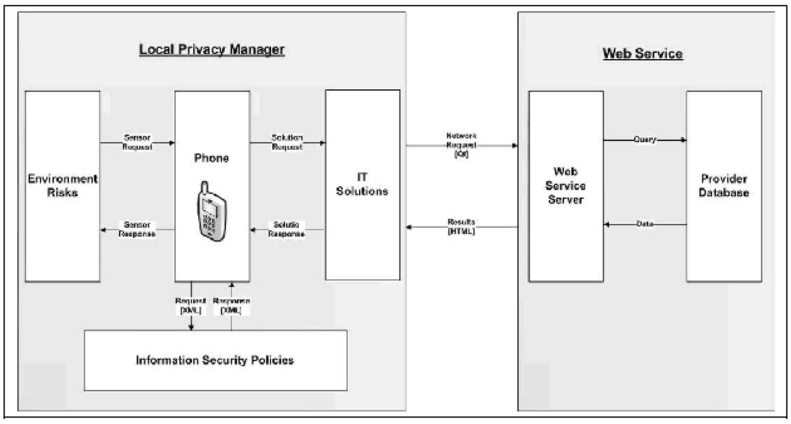


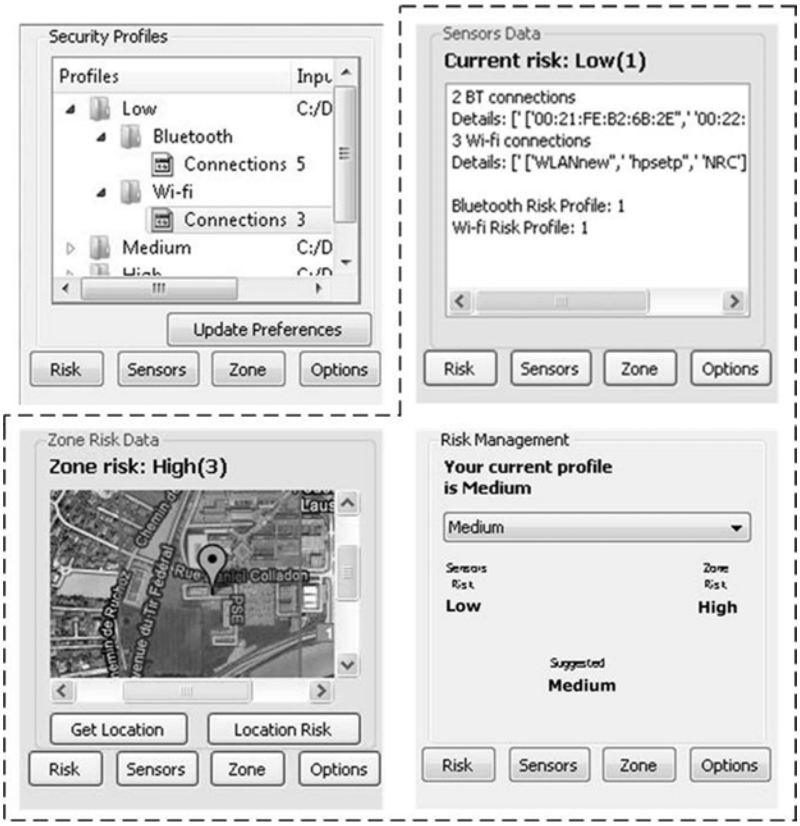
Figure 8.9: System architecture

corresponding proposed privacy policies. For the online Web service, we utilized the PHP and a MySQL based framework, which facilitates the development of dynamic Web applications and allows for the exchange of information with web services. On the client side, the Qt Network Request and Access Manager offers dynamic HTML with integration of Google Maps technologies, which provides localization and auto-update functions, as well as high performance risk degree parsing.

8.3.7 Graphical user interface

The designed application aims at a clear layout and a high degree of user friendliness. For a complete review of the graphical user interface, in the following, we focus on the design of the activity, information and interaction. For the user who is a first time user of this application, a welcome page is proposed and used for the configuration of privacy policies, which explains the purpose and the content of the local risk degree, and its proposed privacy policies on related risk. From this starting page, the user has the option to define the degree of attack for each phone's technology, for example the Bluetooth, Wi-Fi, GPRS and so on. Privacy policies are represented by a list that contains a large related security application which could be selected by the user to enforce the rule that fits the current risk degree. All the information about the status change is stored in a file for future use of compliance checking against privacy policies. If a technology or related security application is not listed in the privacy policies list, users can create a new one at any time. Once the local privacy policies are configured by the user, then the 3 main functions of application of the privacy manager are available for use.

Recalling table 3 we illustrate how to implement the five steps of the decision support for privacy risk management. The first function offers a physical sensor that continuously collects diverse information from the environment. It keeps detecting context information of the technologies of different devices around the user, in order to get an updated context degree of risk in real time, including the technology's name, its MAC address and the specific identification, as well as the number of connections for each technology. In addition, each technology's risk profile is calculated automatically to conform to the user's risk degree configuration. The information of ranking, which represents the average of current risk between all of the technologies detected— is presented at the bottom of the screen. The second function shows the information about zone risk, which includes 2 tasks: displaying the user's current position and obtaining this position's historical risk. When clicking the button "Get location", the phone component GPS (Global Positioning System) will be activated and get the user's current position, including the address information of that latitude and longitude. These position values finally are sent to a Web Service Server by PRIVACY MANAGER. Reverse Geocoding [94] is a service of Google Maps available through our Web Server, which can be used to translate latitude and longitude information into an address. This feature is very important for interactions with the user, since positioning technologies provide coordinate information (i.e. "Latitude = 46.5222, Longitude = 6.583555") which is not meaningful to the end user, and users provide location information in the form of an address (i.e. "UNIL Dorigny, 1015 Chavannes-pres-Renens, Switzerland") which is not useful to software and positioning technologies. Reverse Geocoding bridges the gap between the end user and the positioning technology and enables user interaction with applications, as well as enabling the other types of services by supplying location information to the software in a usable format. For the sake of simplicity, we did not implement a secure connection between the mobile device and the web server even though we adware of its importance. In considering the usability aspects and by involving the users, the map user interface service is added in the Web server. This is the ability to display location information in the form of a map, including landmarks and routes, on the mobile phone screen. This service has various levels of control, we can add or remove certain related features on a map, such as add a polygon or showing a significant marker on the map. Users will also be able to select different map views such as regular, satellite, and hybrid that are integrated on phone screen. Focusing on a zone's risk data sharing, the second button named "location risk" which is set up to allow the phone to contact our online web service to send the information regarding the user's current located risk data to the Web Service Server This web server provides interface to users who authorize to access the application. A database is used to store all information about user's risk. Then the web server will return to the users a risk level which is calculated by the average in a similar area in real time (i.e. each 10 minutes). And here the similar area is defined as a specified area, which is a circumference of a circle with its radius of 500 meters. Finally, the web service will deliver in return the average of the risk degree reported by others users in the same geographic area in an earlier period of time. In order to distinguish the degree of risk in a specific area, an alarm system is integrated, and by using different colors on the map to signify the degree of risk, for example, blue signifies low risk in this area and red signifies high risk. The last function lists the average degree of risk obtained previously, including the sensors risk (risk value from Wi-Fi and Bluetooth) and the zone risk (risk value from current location). PRIVACY MANAGER calculates the average of sensor risk and zone risk, and provides the final risk value to help user make the decision, which will be used to execute the related security applications in order to deal with the current risk.



Sensors Data

Current risk: Low(1)

2 BT connections
Details: [' ['00:21:FE:B2:6B:2E",' '00:22:
3 Wi-fi connections
Details: [' ['WLANnew",' 'hpsetp",' 'NRC']

Bluetooth Risk Profile: 1
Wi-fi Risk Profile: 1

Zone Risk Data

Zone risk: High(3)

Risk Management

Your current profile is Medium

Medium

Sensors Risk **Low**

Zone Risk **High**

Suggested **Medium**

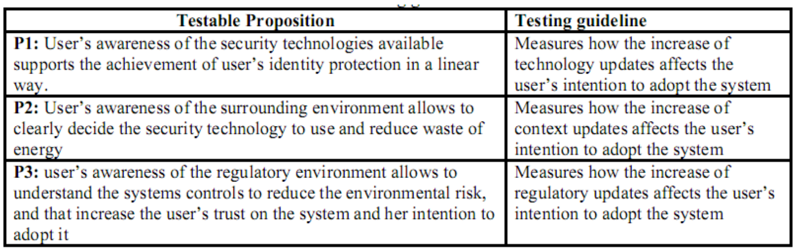
Figure 8.10: The Graphic User Interfaces: Configuration interfaces (top left corner); Sensor analysis interfaces (top right corner); Zone risk analysis interfaces (bottom left corner); Risk management interface (bottom right corner)

8.4 Discussions

A first evaluation has been done within experts in Nokia, to whom the prototype has been presented. Although the idea has been accepted as innovative most of the feedback we received regarding future improvements concerned the user interface and the need to include in the prototype an example of a security enforcing policy. A second evaluation of the prototype has been done within a small sample of mobile users to assess the software usability and the users' intention to use it. We have conducted a pre-test of our prototype using ten volunteers in a controlled environment. Since we cannot perform a benchmark with existing solutions, we opted for a scenario-based test as suggested by Rosson and Carroll [209]. The volunteers were asked to read the two parts of the scenario 8 presented in the previous section. Then they were asked to perform it using an Android mobile phone, on which the Privacy Manager prototype was installed. Since we did not fully implement the security algorithm we simulated that part. At the end of the experience the volunteers were asked to answer questions concerning technology acceptance taken from Vankestesh et al. [244]. The answers we obtained from the volunteers came as partially unexpected. Most users declared they liked the application and they found it useful but that they did not want to use it in their everyday life. It turned out that most users did not feel their privacy menaced and they did not want to be constrained by this kind of application. Yet the same users agreed they might have been exposed to privacy risks and they declared that if the application informs the user of the consequences of each privacy risk, then they would find it useful. Although the sample size does not allow any statistical interpretation, we are currently investigating more in details the underlying causes behind the test results. If they are due to an effect of adverse selection, as suggested by Anderson [7], then this impacts the requirements for software development, since the application should protect and inform the user in the proper way. Moreover it could be that for high maintenance information system for security this statement is not always correct. This point is worth a further analysis, since it would have a significant impact on design requirements.

8.5 Future directions of investigation

In the close future we are going to improve the prototype using the outcome of our preliminary test before testing it on a larger scale using the guidelines illustrated in figure 8.11. Yet we believe that by now our proposed design makes a contribution since it is a first attempt at empowering the user with a system that allows him to manage the dynamically privacy risk according to his own preference and perceptions. Future research directions that we envisage from our work are the following ones: - Extending the model, e.g. adding more contingency factors: in this article we did not take into account other seminal researches, like the five-force model of Porter [186]. - Adding more business models for coopetitve users, e.g. for a distributed infomediary: as previously mentioned the informediary does not have to be a centralized entity. In the extreme case where all the computation is done among mobile users in a distributed fashion the infomediary business model might not work as described here. - Technical improvements for the prototype: a greater amount of effort could be spent analyzing the ways we could improve the human-computer interaction. Security algorithms have to be translated in a common format to be processed by the application, although this has not be done here for technical limitations of the language used. Each protection algorithm has its own limitations. We cite Krumm[133] for a good review of their strengths and weakness, and we suggest reading Shabtai et al. [216] for a security assessment of Android OS.



Testable Proposition	Testing guideline
P1: User's awareness of the security technologies available supports the achievement of user's identity protection in a linear way.	Measures how the increase of technology updates affects the user's intention to adopt the system
P2: User's awareness of the surrounding environment allows to clearly decide the security technology to use and reduce waste of energy	Measures how the increase of context updates affects the user's intention to adopt the system
P3: user's awareness of the regulatory environment allows to understand the systems controls to reduce the environmental risk, and that increase the user's trust on the system and her intention to adopt it	Measures how the increase of regulatory updates affects the user's intention to adopt the system

Figure 8.11: Testing guidelines

8.6 Conclusions

In this paper we have presented a model for decision support system regarding privacy risk management associated with pervasive technologies, which we believe is topic with growing importance in these days. Our research question focused on context-aware technologies used by a user that we assume as opportunistic and rationally bounded. Our theoretical model is the first to take into account the four contingency factors (business, technology, regulation and user behavior) that impacts mobile privacy risk management. We illustrated how our theoretical model allows to benchmark all privacy management applications on the market and to extend such market towards a new type of software. The prototype we developed is the first middleware that combines a transparent and reflective approach, as well as a decentralized (sensor analysis) and centralized (zone risk analysis) risk management mechanism. We followed the methodology proposed by Peffers et al. [182] to structure our design research study, and we used the scenario-based approach of Rosson and Carroll [209] during the development phase. We presented our results to an audience that was a balanced mix of technology-oriented and management-oriented experts at Nokia and we performed over a set of mobile users to assess their intention to adopt our new system. The guidelines for a new round of tests over a larger sample of users have been illustrated in the previous section. This study has some limitations. As the development of fully operational prototype is still ongoing we are currently limited in our results by the application that runs on the phone. However, we believe that our work is well aligned with those who believe that a risk management approach is required to assure information security, and that privacy management in pervasive computing is a complex and multidimensional issue that should be addressed taking into consideration time and place. Our contention is that our model is more flexible than previous ones, since it has been conceived to be updated in time and to mitigate and record threats. Some interesting future researches are envisaged, which might involve privacy risk management in the sector of mobile payment, adding more business models for competitive users, and technical improvements for the prototype.

Chapter 9

Privacy-friendly Business Models for Location-Based Mobile Services

Abstract

This paper presents a theoretical model to analyze the privacy issues around business models for location based mobile services. We report the results of an exploratory field experiment in Switzerland that assessed the factors driving user payoff in mobile business. We found that (1) the personal data disclosed has a negative effect on user payoff; (2) the amount of personalization available has a direct and positive effect, as well as a moderating effect on user payoff; (3) the amount of control over user's personal data has a direct and positive effect, as well as a moderating effect on user payoff. The results suggest that privacy protection could be the main value proposition in the B2C mobile market. From our theoretical model we derive a set of guidelines to design a privacy-friendly business model pattern for third-party services. We discuss four examples to show the mobile platform can play a key role in the implementation of these new business models.

9.1 Introduction

New regulatory requirements and consumer concerns are driving companies to consider more privacy-friendly policies, often conflicting with their desire to leverage customer data. On the one hand access to real intentions and close proximity of potential customers has a real value for mobile location-based service providers, who expect revenues to reach more than $12.7 billion by 2014 [71]. On the other hand implicit in the collection of consumer right of privacy, which we refer as the right to be left alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned. (Black's Law dictionary in [108]). Improper or non-existent disclosure control can be the root cause for privacy issues and privacy personally identifiable information is collected and stored - in digital form or otherwise. Therefore the challenge for companies is to reduce user data collection to the lowest economically sustainable level. Much research to date has focused on understanding the relationship between user privacy concerns and the willingness to disclose personal information to online companies [114, 58]. In this sense user privacy concerns are found to be one major predictor on the willingness to provide personal information. Nevertheless we argue that previous research only focuses on user choice to either withhold or release personal information. This decision is one component of user payoff, which we consider as the degree to which a mobile user perceives as fair the benefits he or she receives in return for the release of personal information [179]. If user's payoff is not assured, data security is in peril [7]. In the rest of the paper we focus on location-based services offered in the Business to Consumer (B2C) market, such as navigation, information, advertising, tracking and billing [90]. We exclude emergency services from our analysis because in those cases users deal differently with privacy concerns [217]. In doing so we primarily address an audience mainly composed of business model designers who seek guidelines to develop privacy-friendly business models. We wish to raise the interest of the broader audience of information system researchers and practitioners who are concerned with the impact of business model practices over the design of the IT artifact [19].

Our research question is: How should a privacy-friendly business model which can sustainably maximize(s) the payoff of a location-based mobile service user be designed?

The remainder of the paper proceeds as follows. In the next section, we review some of the related works in privacy and location based services that address our research question, and we define a set of research sub-questions to fill the remaining gaps. The third section presents the methodology we use to address these sub-questions. The fourth section introduces our theoretical model and presents empirical evidences to support it. In the fifth part, we implement our theoretical model to derive a set of guidelines to obtain privacy-friendly business models. Section six present a set of possible instantiations of our guidelines using real companies as potential candidates. In the last section, we discuss the implications of our analysis and draw some conclusions and propose further possible research.

9.2 Literature review

In this section we briefly highlight a set of well-known works that help us in answering our research question. For a more complete literature review of privacy management technologies, we suggest reading [60]. After outlining the remaining gaps in the literature, we derive a set of research sub-questions that remain to be answered.

The success of the privacy management solution relies on the development of technology and the regulations to protect personal information [6]. Yet privacy is a dynamic and dialectic process of give and take between and among technical and social entities in ever-present and natural tension with the simultaneous need for publicity [179]. Therefore we understand the mobile user and the service provider as both competing and cooperating to gain access to a valuable resource (mobile user data) [163].

Research aimed at surveying and classifying the on-line privacy management solution was also conducted in order to evaluate the different factors and their impact in terms of collaboration [138, 115]. It has been found that different types of privacy assurance have different impacts on people's willingness to disclose personal information – the existence of a privacy statement induces more subjects to disclose personal information, but that of a privacy seal does not [115]. It has also been proved that monetary incentive had a positive influence on disclosure whereas information request has a negative influence suggesting that firms do not collect consumer data unless they intend to use them. In addition to that young English people have more concerns about privacy than French people, resulting in greater perceived risks about data disclosure [138].

Among prior studies focusing on the online business sector, none have examined the specific domain of mobile business settings. Regardless of the fact that there are some similarities between online and mobile businesses, location-based mobile services have their own unique features, which differ from those of online business. Therefore we derive the following research sub-question: R1: What is the specificity of privacy management in the location-based mobile B2C market?

Much research has been consecrated to understanding the relationship between user privacy concerns and their response behaviors in order to design software such as Smokescreen [57]. It reveals that internet user information privacy concerns are a major antecedent of the willingness to provide personal information to online companies. It finds the influences between perceived justice and procedural justice, as well as perceived justice and distributive justice [148, 226].

Previous research has also suggested that control over personal data is an important component in creating a good relationship with customers. Most people want to have more control over the use of personal data to restrict unwanted commercial advertisements [184]. Issues of information control are essential in increasing the likelihood of consumers to contribute information to online firms [229].

Another important issue is the value of personalization. According to [45], service personalization is said to depend on two factors: 1) company ability to acquire and process customer information; and 2) customer willingness to share information and use personalized services. They develop a model to predict consumers' usage of on-line personalization as a result of the tradeoff between their value for personalization and concern for privacy. However, those studies do not provide guidelines for business model designers. Therefore our second research sub-question is: R2: Which business model components allow a high level of mobile user payoff, while keeping the collected data to a minimum?

Finally, comprehensive analyses in consumer privacy concerns and internet related business have proposed [138] four different clusters of users: well-intended, negotiator, unconcerned and reticent. These analyses suggested that when considering the approach to e-commerce, we should also respect the different groups of internet users. Still such results appear to not have strong statistical relevance. Hence our third sub-question is: R3: How should the differences in payoff among privacy risk neutral and privacy risk adverse mobile users be addressed?

In the following section we illustrate how we intend to address our research sub-questions to answer our initial research question.

9.3 Methodology

Based on the relevant literatures, we create an artifact in the form of a model [150] to express the relationship between user payoff and the extent of personal data disclosed. We adopt a design science research methodology, and we refer to existing guidelines for design theories [96]. The theories for design and action give explicit prescriptions on how to design and develop an artifact, whether it is a technological product or a managerial interventio [96]. Therefore, we advance in three steps, as illustrated in 9.1.

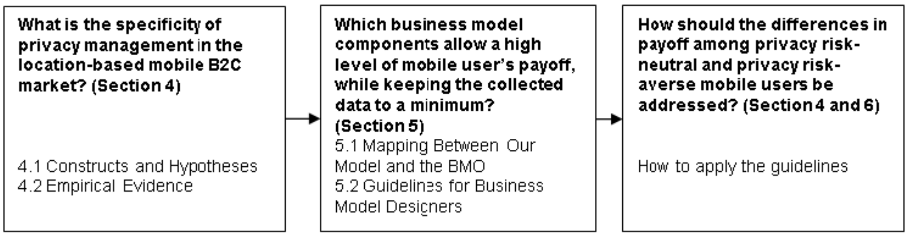

What is the specificity of privacy management in the location-based mobile B2C market? (Section 4)
4.1 Constructs and Hypotheses
4.2 Empirical Evidence
Which business model components allow a high level of mobile user's payoff, while keeping the collected data to a minimum? (Section 5)
5.1 Mapping Between Our Model and the BMO
5.2 Guidelines for Business Model Designers
How should the differences in payoff among privacy risk-neutral and privacy risk-averse mobile users be addressed? (Section 4 and 6)
How to apply the guidelines

Figure 9.1: Our three steps

An information system design theory (ISDT) should define its purpose and scope, i.e. the boundaries of a theory. In our case our theory concerns data management for privacy risk reduction of location-based services. The second element of an ISDT is the representations of the entities of interest in the theory, i.e. constructs. The principles of form and function define the structure, organization, and functioning of the design product or design method. The justificatory knowledge provides an explanation of why an artifact is constructed as it is and why it works.

Accordingly in section 4 we introduce a model composed of four constructs and make hypotheses on the interaction among constructs. In doing so we ground our claims on existing theories of control [64], as well as perceived justice and equity theory (used in [226]).

The evaluation strategy of testable propositions uses surveys as an ex-post artificial type of evaluation [189]. The resulting outcomes provide answers to the first sub-question.

Our second sub-question concerns the means by which the design is brought into being—a process involving agents and actions. To do so section 5 starts by mapping our constructs with the constructs of the Business Model Ontology (BMO) [175], a tool often used by startups and multinational companies to represent their business model. Since our model has only four constructs and the BMO is composed of 9 elements, we rely on an existing type of business model (the infomediary pattern) to fill in the blanks and derive a set of guidelines for business model designers to obtain privacy-friendly business models.

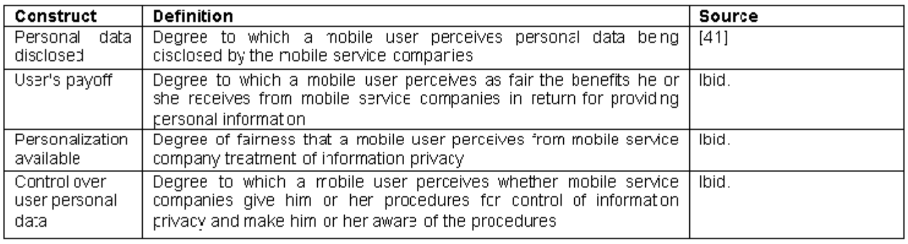
To properly answer our third sub-question we need to test the feasibility of the proposed guidelines. Hence section 6 presents a set of instantiations of our business model pattern. While a theory is an abstract expression of ideas about the phenomena in the physical world, instantiated artifacts are things in the physical world. Thus we illustrate four examples of application for our guidelines naming four existing companies as possible candidates. This gives us the opportunity to describe how flexibility and adaptability may be enabled by feedback loops to refine design towards either a centralized or a decentralized privacy-friendly business model.

9.4 Model

In this section we present our theoretical model following the guidelines to describe a theory [231]. We start by presenting the constructs and by augmenting our hypotheses using the references we introduced in the literature review. Then we show the correlations among components, which we derive from our test results.

9.4.1 Constructs and hypotheses

Our model is composed of four constructs, the definitions of which are derived from previous research summarized in figure 9.2.



Construct	Definition	Source
Personal data disclosed	Degree to which a mobile user perceives personal data being disclosed by the mobile service companies	[41]
User's payoff	Degree to which a mobile user perceives as fair the benefits he or she receives from mobile service companies in return for providing personal information	Ibid.
Personalization available	Degree of fairness that a mobile user perceives from mobile service company treatment of information privacy	Ibid.
Control over user personal data	Degree to which a mobile user perceives whether mobile service companies give him or her procedures for control of information privacy and make him or her aware of the procedures	Ibid.

Figure 9.2: Definitions of each construct of our model

Since previous studies have already focused on the effects of antecedents, we focus on the effects among antecedents. We refer to [226] and we claim that the degree to which a mobile user perceives as fair the benefits he or she receives from mobile service companies in return for providing personal information" (i.e. user payoff in our model) is found to be one major predictor for the personal data disclosed, which we define as the degree to which a mobile user perceives whether personal data is disclosed by the mobile service company. Therefore, we propose a model of user payoff as indicated in figure 9.3: H1: The personal data disclosed has a negative effect on user payoff.

In exchange for user data, the m-commerce provider could offer a service, which is either standard or fully customized. We introduce the concept of service personalization, which we define as the degree of fairness that a mobile user perceives relative to mobile service company treatment of information privacy. As we previously mentioned in the literature part, service personalization depends on customer willingness to share information and use personalized services [45]. It is natural to expect a positive relationship between the amount of personalization available and users benefit. H2: The amount of personalization available has (a) a direct and positive effect and (b) a moderating effect on user payoff.

Since consumers take relatively high risks by submitting personal data to the mobile service provider, data controls using privacy metrics [108] are a useful tool to decrease user concern for privacy risks. Lack of such control decreases mobile user trust in the provider [64] and lowers the perceived payoff. Hence we propose that: H3: The amount of control over user personal data has (a) a direct and positive effect and (b) a moderating effect on user payoff.

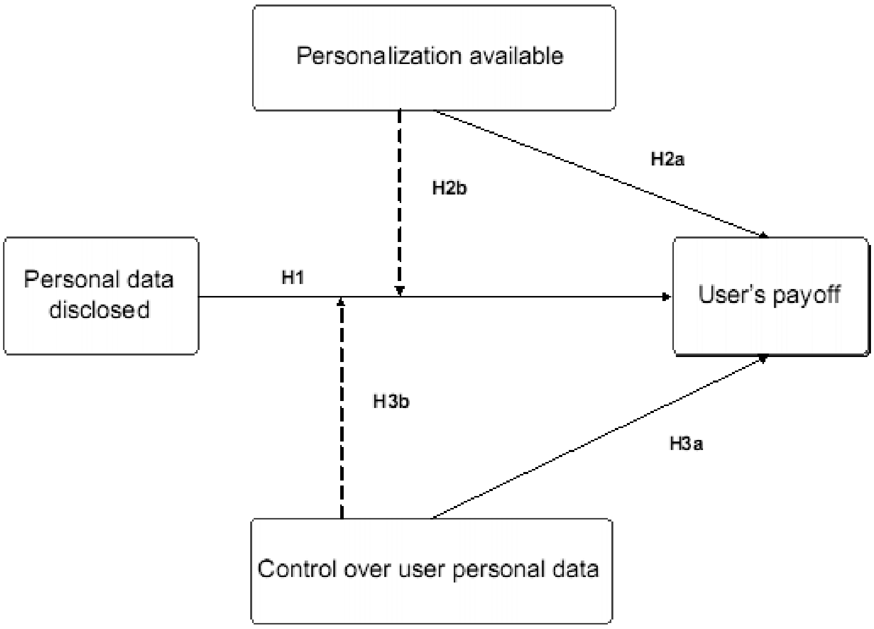


Figure 9.3: Model of user payoff

9.4.2 Test design

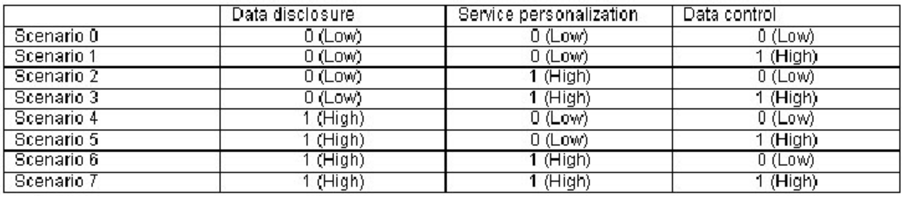
In our study we want to test the effect of the data disclosure, service personalization and data control over user payoff. We test the effect of such constructs in two steps. Since we are mostly dealing with perceptions, we test the effect of our model using scenario based surveys. This form of assessment has been successfully implemented in previous studies on information system security [15].

As illustrated in the figure 9.4 we designed two at the power of n different scenarios, where n is the number of constructs in our model that we want to test, and 2 is the value that each construct can get (0=Low or 1=High). All subjects are to receive scenario 0, which test the initial user's payoff:

"Your mobile phone operator (e.g. Swisscom) offers you a new service – a discount zone. With this service, you can get exclusive information and access to exclusive personal time and location limited discounts on a diversity of products and services (e.g., books, pizzas, electronics, cinema, etc.) near your current location. For example, if you are interested in acquiring an iPad, Swisscom will automatically send a SMS to your mobile phone when there is a special and exclusive discount for iPads near your location.

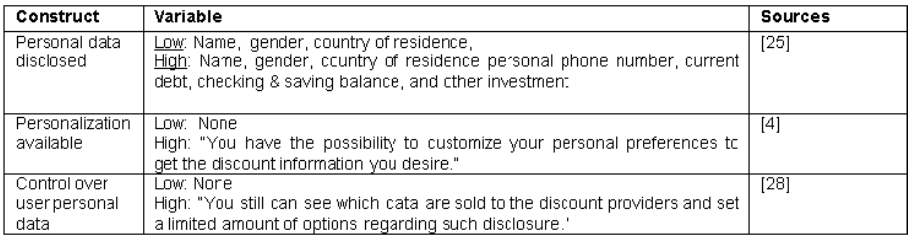
There are two ways to register for this service: a paid yearly subscription which gives access to the full service or a free registration. To get free registration you must provide additional information, including your name, gender, country of residence. Your data is stored according to privacy laws and sold to discount providers. "

Then we split the overall sample in sub-groups. Each sub-group gets a variation of the initial scenario and it is asked to express the new user's payoff.



	Data disclosure	Service personalization	Data control
Scenario 0	0 (Low)	0 (Low)	0 (Low)
Scenario 1	0 (Low)	0 (Low)	1 (High)
Scenario 2	0 (Low)	1 (High)	0 (Low)
Scenario 3	0 (Low)	1 (High)	1 (High)
Scenario 4	1 (High)	0 (Low)	0 (Low)
Scenario 5	1 (High)	0 (Low)	1 (High)
Scenario 6	1 (High)	1 (High)	0 (Low)
Scenario 7	1 (High)	1 (High)	1 (High)

Figure 9.4: Our scenarios

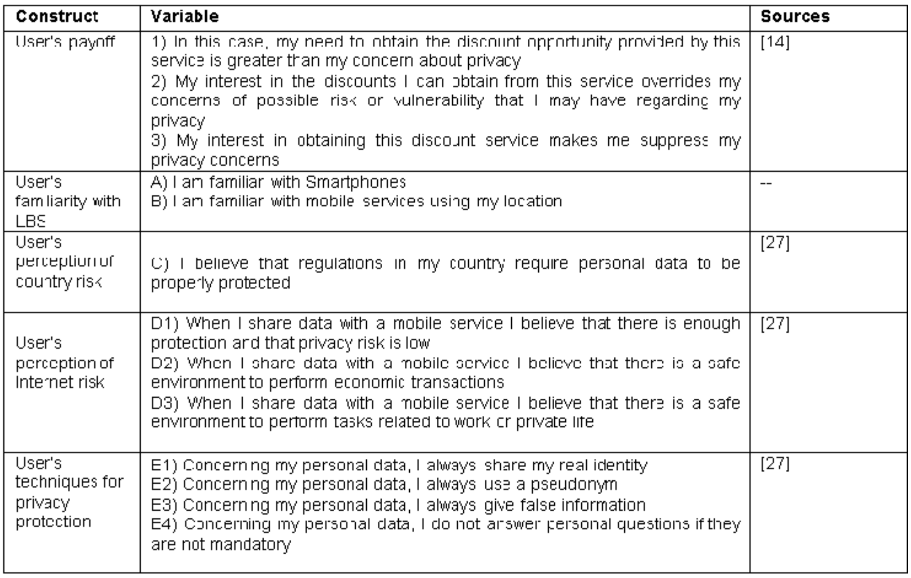


Construct	Variable	Sources
Personal data disclosed	Low: Name, gender, country of residence, High: Name, gender, country of residence personal phone number, current debt, checking & saving balance, and other investment	[25]
Personalization available	Low: None High: "You have the possibility to customize your personal preferences to get the discount information you desire."	[4]
Control over user personal data	Low: None High: "You still can see which data are sold to the discount providers and set a limited amount of options regarding such disclosure."	[28]

Figure 9.5: Operationalization of constructs for the scenarios

As figure 9.5 indicates, each variation of the scenario operationalizes one construct of our model, and it is derived from previous works.

To measure the user's payoff we derive three items from previous studies. A set of control variables are included as well, as shown in figure 9.6.



Construct	Variable	Sources
User's payoff	1) In this case, my need to obtain the discount opportunity provided by this service is greater than my concern about privacy 2) My interest in the discounts I can obtain from this service overrides my concerns of possible risk or vulnerability that I may have regarding my privacy 3) My interest in obtaining this discount service makes me suppress my privacy concerns	[14]
User's familiarity with LBS	A) I am familiar with Smartphones B) I am familiar with mobile services using my location	--
User's perception of country risk	C) I believe that regulations in my country require personal data to be properly protected	[27]
User's perception of Internet risk	D1) When I share data with a mobile service I believe that there is enough protection and that privacy risk is low D2) When I share data with a mobile service I believe that there is a safe environment to perform economic transactions D3) When I share data with a mobile service I believe that there is a safe environment to perform tasks related to work or private life	[27]
User's techniques for privacy protection	E1) Concerning my personal data, I always share my real identity E2) Concerning my personal data, I always use a pseudonym E3) Concerning my personal data, I always give false information E4) Concerning my personal data, I do not answer personal questions if they are not mandatory	[27]

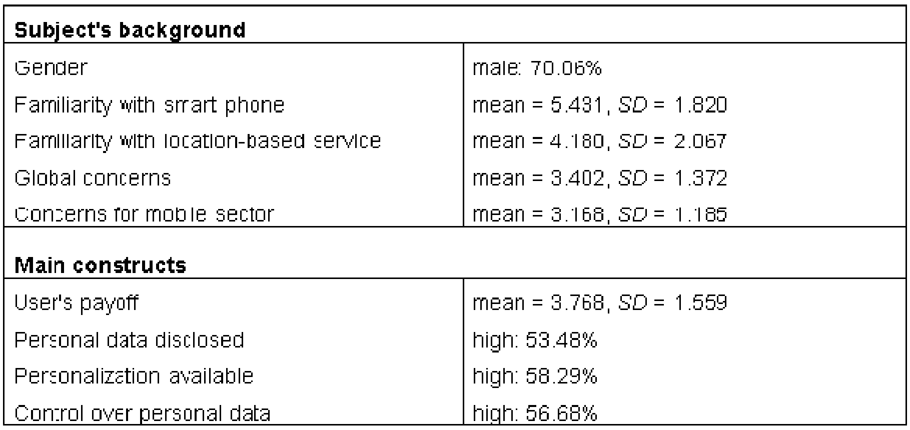
Figure 9.6: Operationalization of variables for the survey

9.4.3 Results

We invited a group of subjects to fill out a survey concerning privacy issues in a location-based mobile service context. The descriptive statistics of the sample are presented in figure 9.7. Our sampling frame consisted of 187 bachelor students at the business faculty of a Swiss university, who attended the course in information system. The sample was chosen due to the expected likelihood that the population of smart-phone mobile users in Europe.

The subjects were between 19 to 24 years old, with 70 percent of sample being male. This well relates with the recent figures on smart phone users in Europe: 27% between 16 and 24 years old and 67% male, according to Forrester Research, Inc [117].

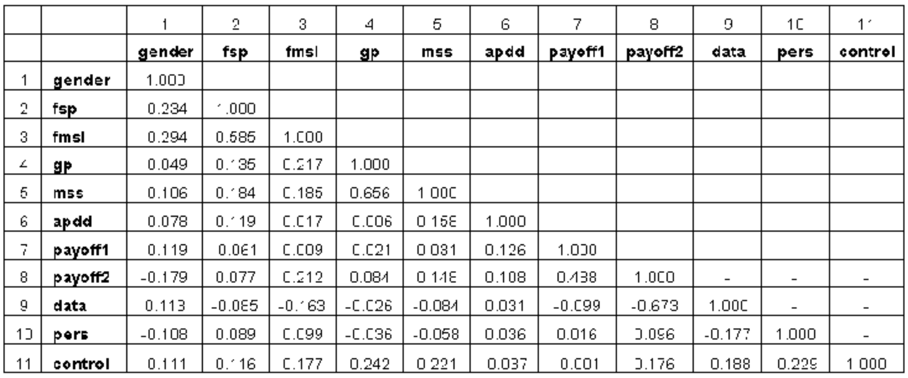
From previous research we derived two items to test for cultural effect. We can compare to English [138] that had the same sample distribution.



Subject's background	
Gender	male: 70.06%
Familiarity with smart phone	mean = 5.431, *SD* = 1.820
Familiarity with location-based service	mean = 4.180, *SD* = 2.067
Global concerns	mean = 3.402, *SD* = 1.372
Concerns for mobile sector	mean = 3.168, *SD* = 1.185
Main constructs	
User's payoff	mean = 3.768, *SD* = 1.559
Personal data disclosed	high: 53.48%
Personalization available	high: 58.29%
Control over personal data	high: 56.68%

Figure 9.7: descriptive statistics

In figure 9.7 can be seen information on the correlation coefficients between all used constructs. We observe a relatively high correlation coefficient between global concerns for privacy and concerns in the mobile service sector (0.656). Since both variables deal with attitude to privacy risks, it is natural to expect a positive linkage between them. We did not otherwise observe any significant proof of multicollinearity effects among our variables.



		1	2	3	4	5	6	7	8	9	10	11
		gender	**fsp**	**fmsl**	**gp**	**mss**	**apdd**	**payoff1**	**payoff2**	**data**	**pers**	**control**
1	**gender**	1.000										
2	**fsp**	0.234	1.000									
3	**fmsl**	0.294	0.585	1.000								
4	**gp**	0.049	0.135	0.217	1.000							
5	**mss**	0.106	0.184	0.185	0.656	1.000						
6	**apdd**	0.078	0.119	0.017	0.006	0.158	1.000					
7	**payoff1**	0.119	0.061	0.009	0.021	0.031	0.126	1.000				
8	**payoff2**	-0.179	0.077	0.212	0.084	0.148	0.108	0.438	1.000	-	-	-
9	**data**	0.113	-0.065	-0.163	-0.026	-0.084	0.031	-0.099	-0.673	1.000	-	-
10	**pers**	-0.108	0.089	0.099	-0.036	-0.058	0.036	0.016	0.096	-0.177	1.000	-
11	**control**	0.111	0.116	0.177	0.242	0.221	0.037	0.001	0.176	0.188	0.229	1.000

Figure 9.8: Correlation among constructs

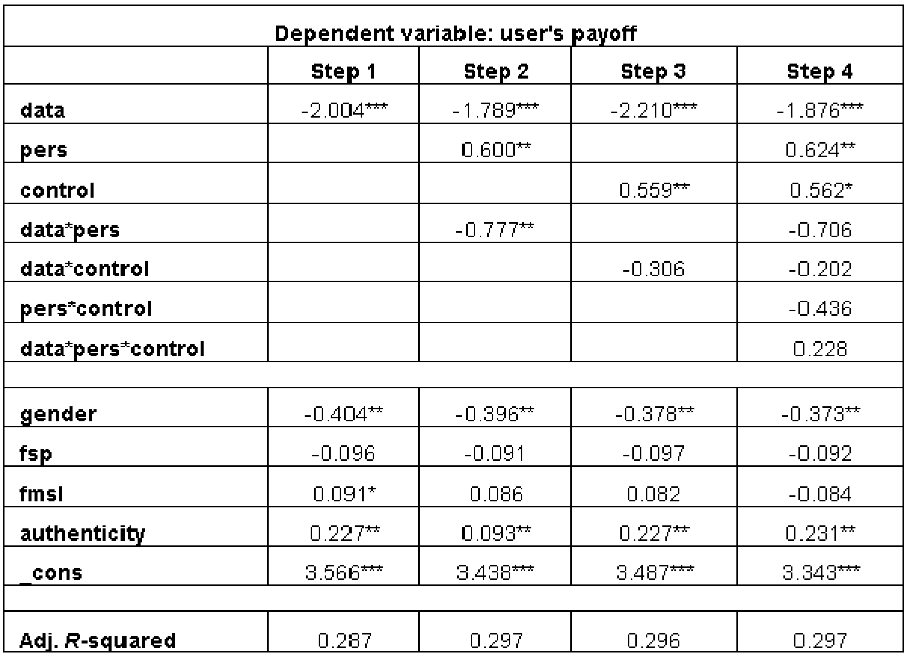
[Notes for figure 9.8 fps: familiarity with smart phone; fmsl: familiarity with mobile services using my location; gp: global concerns for privacy; mss: concerns in mobile service sector; apdd: authenticity of personal data disclosed; payoff1: user payoff in scenario 0 (base scenario); payoff1: user payoff in other scenarios; data: personal data disclosed; pers: personalization available; control: control over personal data.]

To test the relationships between variables, we conducted several regression tests using the statistical software STATA 9. The ANOVA test proves that there is no significant effect of scenario 0 over payoff: F(6,164) = 0.83, p = 0.547, adj R2 = -0.0057. Therefore we include this control group in our final model. Accordingly, the sample size doubles in the regression equations. The results shown in figure 9.8 presents the outcomes of our four steps. In all regression models, the dependent variable is user payoff.

In the first step, we simply focus on the impact of data disclosed. We introduce control variables such as gender, familiarity with smart phones, as well as user's familiarity with location-based services and authenticity of disclosed data.

In the second step, we add personalization available as another main independent variable. We also consider the potential interaction effect between the new variable and data disclosed, which we named "data*pers". The third step concerns the control over personal data, and the interaction between data and control (data*control). The final step includes all these three main independent variables and their interactions. The results are shown in figure 9.9.

For each step we measured the adjusted R squared, as figure 9.9 indicates whether the inclusion of additional variables increased the overall explanatory power of the model.



Dependent variable: user's payoff				
	Step 1	Step 2	Step 3	Step 4
data	-2.004***	-1.789***	-2.210***	-1.876***
pers		0.600**		0.624**
control			0.559**	0.562*
data*pers		-0.777**		-0.706
data*control			-0.306	-0.202
pers*control				-0.436
data*pers*control				0.228
gender	-0.404**	-0.396**	-0.378**	-0.373**
fsp	-0.096	-0.091	-0.097	-0.092
fmsl	0.091*	0.086	0.082	-0.084
authenticity	0.227**	0.093**	0.227**	0.231**
_cons	3.566***	3.438***	3.487***	3.343***
Adj. *R*-squared	0.287	0.297	0.296	0.297

Figure 9.9: regression models

Notes for figure 9.9: *p¡0.1; **p¡0.05; *** p¡.01;

As figure 9.9 indicates, the extent of data discolsed always has a significant effect on user payoff (p¡0.01 in all four steps), which is negative (-2.004 in the first step). In other words, it appears that mobile users sacrifice certain benefit or increase their concerns for risk, when the service asks for their personal information. Thus H1 is strongly supported.

Service personalization has a significant effect on user payoff (p¡0.05 in step 2 and 4), which is positive (0.600 in step 2). This fits well with previous research [226], which found a value of 0.60 as well. Interestingly we find a significant negative interaction effect of personalization on the relationship between data disclosed and payoff (-0.777 in step 2), though such an effect is not strongly significant (p¿0.05 in step 2 and 4). Thus H2a is supported but H2b is not supported.

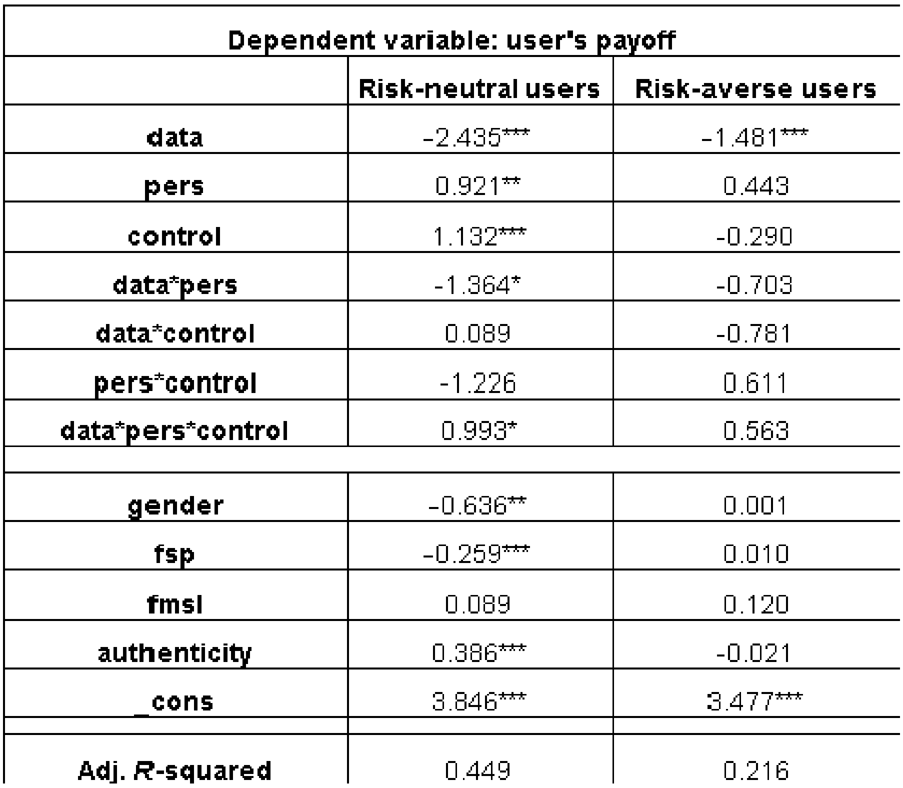
Control has a positive (0.599 in step 3) effect on user payoff, although there is not always a relevant significant effect on user payoff (p¡0.05 in step 3; p¡0.01 in step 4). We found no relevance for the moderating effect of control over user payoff with the whole sample. Therefore, H3a is weakly supported and H3b is not supported.

Recalling [138], we confirm that gender was an effect on user's payoff. We also expect that people who show general low risk awareness have different opinions on their payoffs as opposed to those who are highly risk averse. Thus we divide our sample into two clusters accordingly. We adopt median cluster method based on two variables: subjects' global concerns for privacy and concerns in the mobile service sector. We exclude sample observations that are equal to the value of median. We conduct regression analysis for both clusters, and the results are indicated in figure 9.10.

We find that for people who have a relatively high level of concern about privacy when providing personal information (risk-averse users), neither personalization available nor user control over personal data plays an important role in determining payoff this interpretation extends previous analysis on why privacy policies on website are often not shown in the first page [30]. For people who have a relatively low level of concern about privacy when providing personal information (risk-neutral users), both variables are demonstrated to be essential indicators. In the last column of figure 9.10, we observe that the only variable that has a significant impact on payoff is data (-1.481, p ¡ .01). Hence, H2 and H3 are rejected for risk-averse mobile users. However, there are significant effects of personalization available and user's control for risk-neutral users. In particular, personalization being available has a significant positive direct impact on user payoff (0.912, p ¡ .05) and a significant negative moderating effect on the relationship between personal data disclosed and user payoff (-1.364, p ¡ 0.1). User's control over personal data has a strong positive impact on user's payoff (1.132, p ¡ .01). Thus, for risk-neutral mobile users, H2 and H3a are supported.

There is also a moderating effect of users control on the relationship between personal data disclosed and user payoff, but such an effect is not significant. Hence H3b is not supported for risk neutral mobile users. We also observe from figure 9.10 that adjusted R squared is 0.449 for risk neutral mobile users, indicating that the overall explanatory power of the model is increased within this group as opposed to that includes all observations (figure 9.9).

In figure 9.11, we describe our results demonstrate that although there is always a tradeoff between user payoff and the extent of personal data disclosed, other factors play different roles on user payoff across different groups of customers.



Dependent variable: user's payoff		
	Risk-neutral users	Risk-averse users
data	-2.435***	-1.481***
pers	0.921**	0.443
control	1.132***	-0.290
data*pers	-1.364*	-0.703
data*control	0.089	-0.781
pers*control	-1.226	0.611
data*pers*control	0.993*	0.563
gender	-0.636**	0.001
fsp	-0.259***	0.010
fmsl	0.089	0.120
authenticity	0.386***	-0.021
_cons	3.846***	3.477***
Adj. *R*-squared	0.449	0.216

Figure 9.10: Regression for risk neutral and risk adverse users

9.5 Implementation of the theoretical model: the trusted infomediary pattern

In this section we derive guidelines to design privacy-friendly business models. We choose to use the Business Model Ontology [175] to represent the theoretical model tested in the previous section. Then we complete the business model of a third party agent, which has a value proposition structure around privacy protection, using the description of an infomediary [101].

9.5.1 Mapping our model on the business model ontology (BMO)

A business model canvas or ontology (BMO) can be described by looking at a set of nine building blocks. These building blocks were derived from an in-depth literature review of a large number of previous conceptualizations of business models. In this depiction, the business model of a company is a simplified representation of its business logic viewed from a strategic standpoint (i.e. on top of Business Process Modeling), which can be seen in detail in figure 9.12.

At the center there is the Value Proposition. It describes which customer problems are solved and why the offer is more valuable than similar products from competitors (product, service). Previous studies have already related perceived customer value to privacy risk[50].

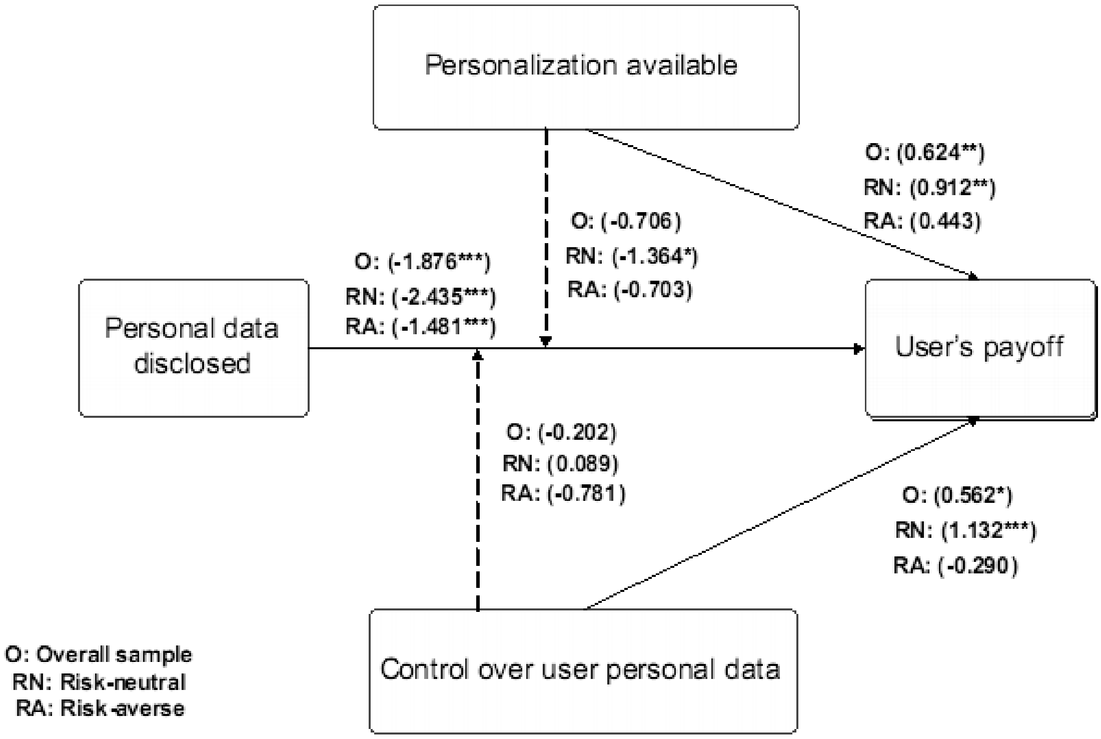


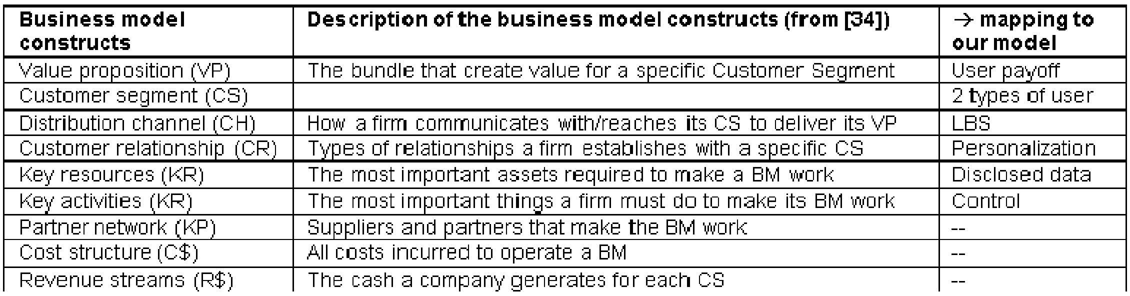
Figure 9.11: Test Model of user payoff

The customers themselves are analyzed in the Customer Segment, separated into groups to help identify their needs, desires and ambitions (singles, families). In our model, there are two types of mobile users, indentified as customer segments: those neutral in respect to privacy risk (52% of the tested sample) and those adverse to privacy risk (48% of the tested sample). Thus the value proposition can be derived by the user's payoff: the risk neutral users seek personalized service whereas the risk adverse users seek data control.

Distribution Channel illustrates how the customer wants to be reached and by whom (Internet, store). The boundary conditions of our model define that it applies to Location-Based Services; therefore the distribution channel can be considered to be a mobile device with location-based services.

Customer Relationship specifies the type of relationship the customer expects and how it should be established and maintained (promotion, support, individual or mass). Our model has a construct concerning service personalization that maps well to this business model component. To be able to deliver the value proposition, the business has to have Resources (staff, machines, secret knowledge), which in our model is the disclosed data of the user. The firm transforms these resources through Key Activities into the final product or service (development, production, secret process). The construct concerning data control of our model seems to fall into this category.

Figure 9.13describes how our model maps with the BMO. The numbers on the arrows refer to the values we obtained in figure 9.10. According to figure 9.13, the segment of privacy risk–neutral users seeks personalized service composed of a personalized customer



Business model constructs	Description of the business model constructs (from [34])	→ mapping to our model
Value proposition (VP)	The bundle that create value for a specific Customer Segment	User payoff
Customer segment (CS)		2 types of user
Distribution channel (CH)	How a firm communicates with/reaches its CS to deliver its VP	LBS
Customer relationship (CR)	Types of relationships a firm establishes with a specific CS	Personalization
Key resources (KR)	The most important assets required to make a BM work	Disclosed data
Key activities (KR)	The most important things a firm must do to make its BM work	Control
Partner network (KP)	Suppliers and partners that make the BM work	--
Cost structure (C$)	All costs incurred to operate a BM	--
Revenue streams (R$)	The cash a company generates for each CS	--

Figure 9.12: Mapping with the BMO

relationship and a control over personal data. The other segment of mobile users (i.e., the privacy risk–averse) looks for privacy risk mitigation, which can be obtained by a service that collects few personal data.

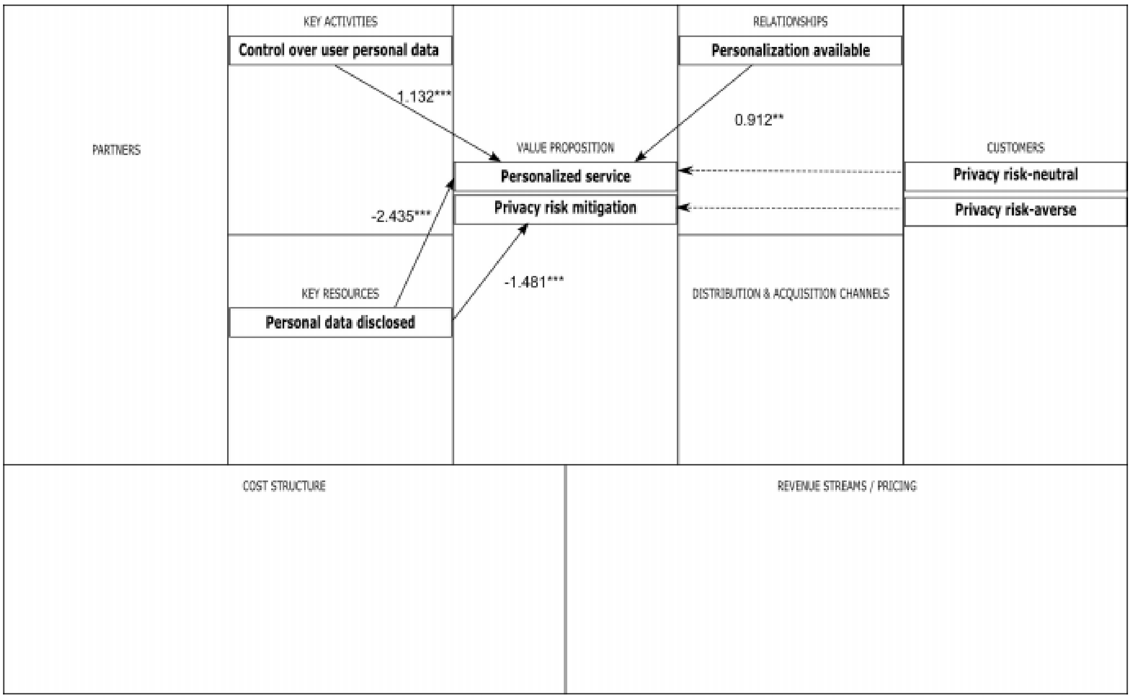


Figure 9.13: The theoretical model represented using the BMO

Most businesses also depend either for resources or for activities on an external Partner Network (logistics, financial), which can provide better quality or a lower price on non essential components. And any business model would not be complete without financial information. Hence the last two building blocks focus on cost and revenue: Cost Structure which should be aligned to the core ideas of the business model (key resources, key activities) and Revenue Streams which mirror the value the customers are willing to pay and how they will perform the transaction (one time fee, subscription).

These elements happen to be missing in our model. In the next section, we obtain a profitable business model by referring to existing business model patterns.

9.5.2 Applying the BMO to derive a privacy-friendly business model pattern

A pattern is commonly referred to as a solution for a problem in a recurring context. Using the business model ontology one can represent a set of business model patterns [175]. Each business model pattern addresses a different goal. It assigns values to components of a business model and specifies relationships to be applied to similar contexts.

For our purposes in 9.14 we introduce the pattern of the infomediary as a special case of multi-sided business model [75]. Infomediary is a term invented by John Hagel and Marc Singer [101]. It was previously referred to as "boundary spanner" or "information broker" and adapted to the e-business. The infomediary is a trusted third party, which helps consumers and vendors connect. The role of our infomediary is to become the custodian, agent and broker of customer information.

The third party has distinct sets of client segments, which need each other, and which cannot get together easily on their own. The infomediary helps them connect through a specific platform. The main cost of a double-sided business is maintaining and developing the platform. As for the revenues, one segment can be subsidies in order to generate enough interest for the platform from the second party which will then pay for the service.

9.14 illustrates the effects of the infomediary pattern introduction on the components of our business model, which we describe here in detail.

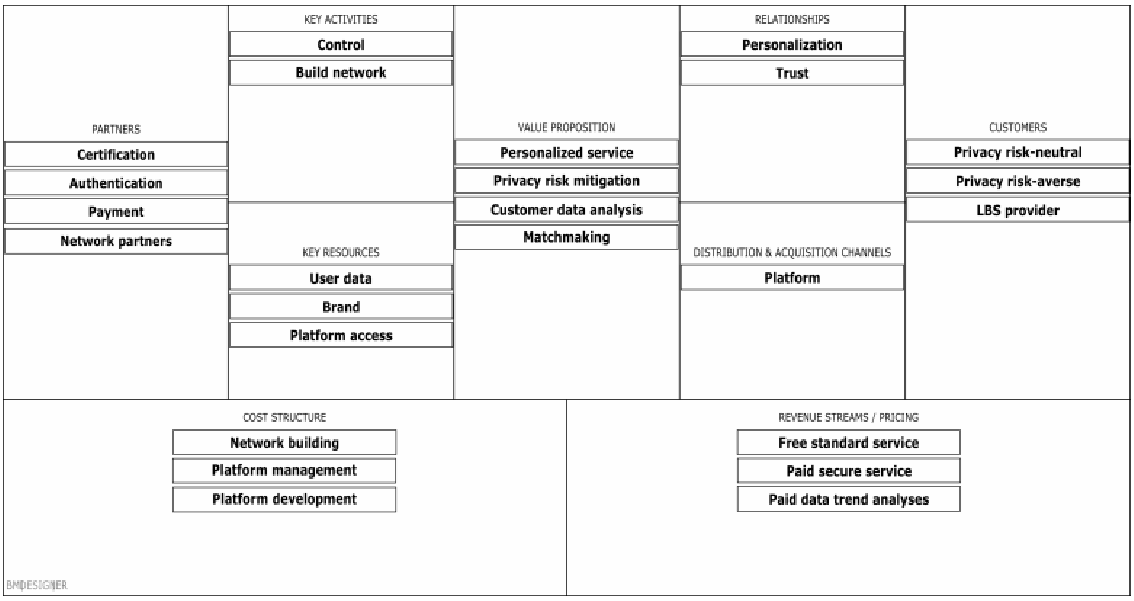


Figure 9.14: Business model for privacy as value proposition

Customer segments: A third customer segment is added to the two existing ones: M-commerce service providers willing to add privacy management to their services to differentiate their offer or tap into the pool of risk adverse users.

Value proposition: According to the three different customer segments we identify three main value propositions:

- Service personalization for privacy risk neutral users: By aggregating customers with the same interest, the infomediary can negotiate better deals. The user only receives advertisements based on personal opt-in profile. The user can get better recommendation based on that individual's personal protected aggregated profile. The user can opt-in to receive certain advertisements, in some cases even get paid for exposing parts of personal detailed profile.
- Privacy risk mitigation for privacy risk adverse users: the infomediary acts as a proxy for the transactions and the delivery in order to hide the customer from the business. The LBS provider's data profiling is minimized the user's data collection for LBS service is reduced. The third party also displays reports on user profile as an overview of the collected information a business rating to help the customer choose services.
- Customer data analysis for LBS providers: trend analyses of privacy risk neutral users can be exchanged with LBS provider for money. And to its service provider segment: Customer acquisition (match): Customer can find the service offered by the business in the infomediary's repository of partners. Marketing (publish to segment): For users who opted-in, the infomediary can forward target advertisements on behalf of a business. In return, the business gets a better return on advertisements since all the recipients should theoretically be in the target segment. Market research (benchmark): the aggregated information gives the possibility to compare results.

Matchmaking among different customer segments is an additional value proposition, which distinguishes the multisided business model pattern.

Customer Relationships: The key to attracting risk adverse users is to promote the importance of privacy protection, as well as building a very strong trust relationship with the customer. The privacy agent has to show users that it knows the high value a user has for personal data and prove it cares a great deal for keeping the data safe. This relationship is very similar to that of a bank and its customers and one way to achieve this is by being transparent. For the risk neutral users a personalized service increases user's payoff.

Channels: Service can be personalized either by means of a platform, which could be either an application of the mobile devices or Internet. For the risk adverse, user's data can be stored in a safe and remote database and retrieved by secure connection.

Revenue Streams: The risk neutral users get the services for free, to gain from the freemium effect. LBS providers pay for risk user data trend analyses, which is the greatest part of the third party income. Risk adverse users are more likely to pay to get their service and so they subsidize the controls offered to the risk neutral users.

Key Activities: The key activity of a mutli-sided business model is to build and promote a network of users of its platform. To assure compliance to the users' policies, the privacy risk can be mitigated by implementing and maintaining a set of controls according to security frameworks such as CobiT and ISO 270001 together with privacy guidelines [166].

Key Resources: The most important element for the third party is user data and access control to the data sharing platform. An additional resource is represented by the brand value, which allows a trusted relationship with the three customer segments.

Key Partners: The third party has to be audited and certified by an external partner. The third party also has to have partnerships with mobile device manufacturers or network operators in order to realize and deploy the product (Network Partners). To offer additional services or implement additional privacy protection, the third party might also need to be in relationship with identity and payment providers.

Cost Structure: Network building and Platform Management and Development activities are costly services.

The third party can always be circumvented by mobile users interacting directly with the LBS provider. But these providers implement privacy only by policy. LBS provider promises not to abuse the data, whereas the third party can implement real privacy by architecture through the platform.

9.6 Business model instances of the trusted infomediary pattern

There is a range of possibilities for technical implementation of privacy protection, intended here as algorithms, data storage and policies. Centralized personalization is seen by some researchers as a major trend in the telecommunications world, whereas others expect most of the personalization to take place on the end-user terminal for reasons of usability, response time and privacy [68].

The literature review of the last ten years of research in privacy-enabling technologies done by [60] allows assessment of the limits of a trusted third party and supports a claim that it is possible to "crowd source" both identity provision and attribute certification [259]. However this approach does not fully explain how to get rid of a trusted third party. Hence, we consider a combination of centralized and decentralized privacy control solutions. Figure 9.15 shows the centralized and decentralized implementations of privacy protection. Different customization degrees of the (centralized) IT infrastructure of the service provider and of the (decentralized) software on user's mobile device are illustrated. This way, we obtain four possible outcomes in our matrix, which we illustrate by using four possible market players as examples.

Alliances among parties can maximize their payoff by cooperating although they have diverging goals [60]. On the one hand a firm that cannot avoid this kind of co-opeting relationship in non-core competence areas can best adapt by decentralizing the largest amount of information collected and by letting other firms do most of the key activities. On the other hand a firm that cannot avoid this kind of relationship in core competence areas can best adapt by centralizing information about the relationship through establishing an inter-organizational structure (the platform) to share information.

9.6.1 Privacy broker

Figure 9.16 illustrates the business model adaptations required for the privacy broker. Mobile network operators such as Nokia are good candidates for deploying a privacy broker since they already possess location information and have direct access to the telecommunication infrastructure. For Mobile network operators, location-based services

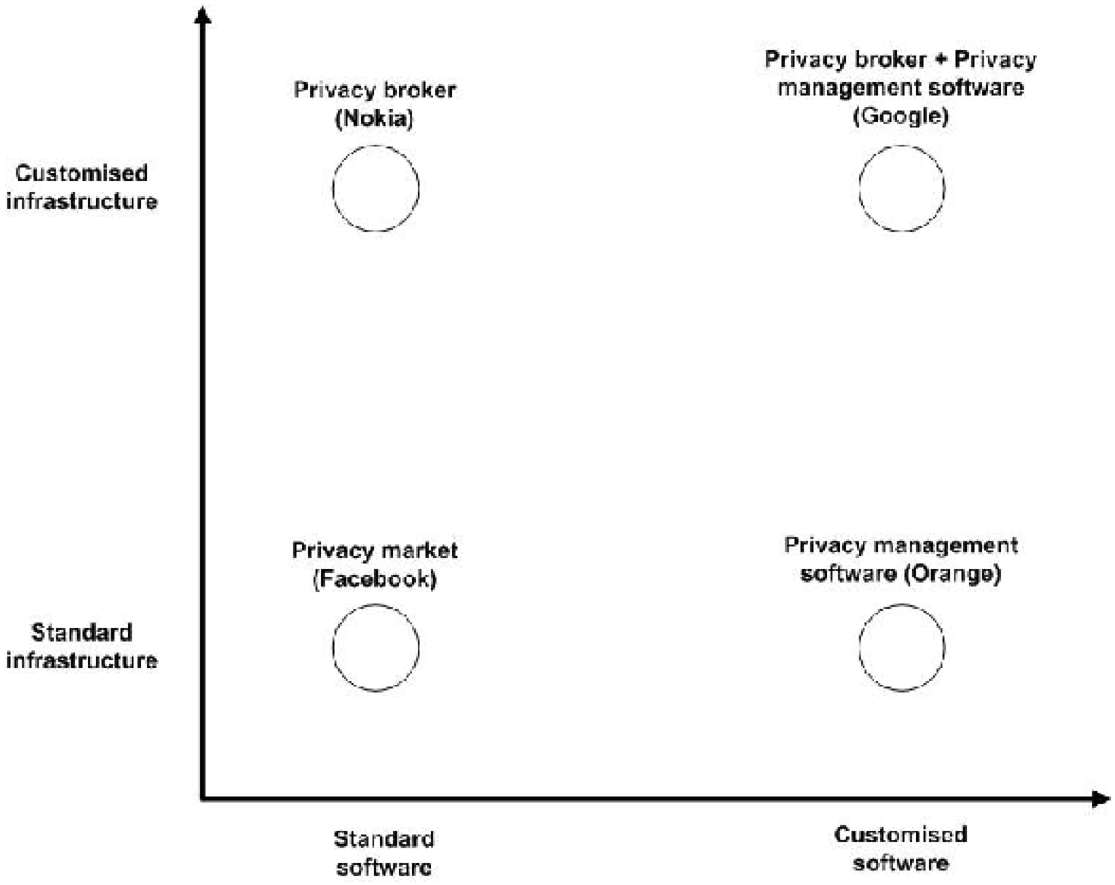

Privacy broker (Nokia)
Privacy broker + Privacy management software (Google)
Customised infrastructure
Privacy market (Facebook)
Privacy management software (Orange)
Standard infrastructure
Standard software
Customised software

Figure 9.15: Instances of privacy-friendly business model

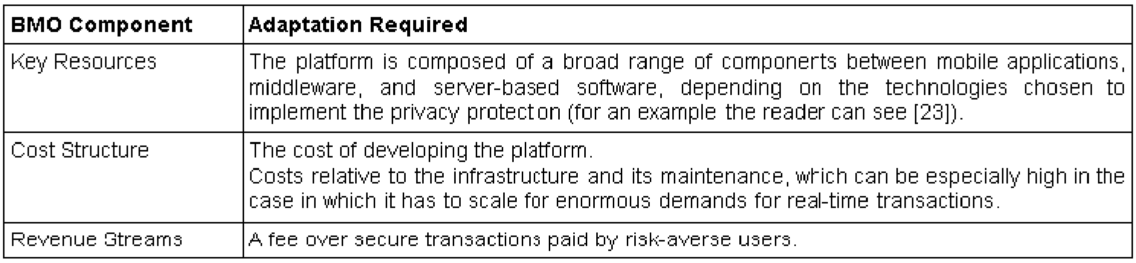
represent an additional stream of revenue generated from their investments in fixed infrastructure[198].

For GPS-enabled terminals, the location of the intelligence shifts towards the handset. This may reduce the role of operators and increase the opportunities for service providers, as accurate location-based information becomes available at no cost. Therefore, adding privacy protection services can become a key differentiator for mobile network operators [68].

Over half of users would be happy if their CSP (Communication Service Provider) would fulfill the role of supervising permission policies [166]. Moreover, providing new LBS like location sensitive billing might be a very attractive aspect of current phone billing possibilities. The biggest difficulty is the creation of relationships with m-commerce providers.

9.6.2 Privacy manager software

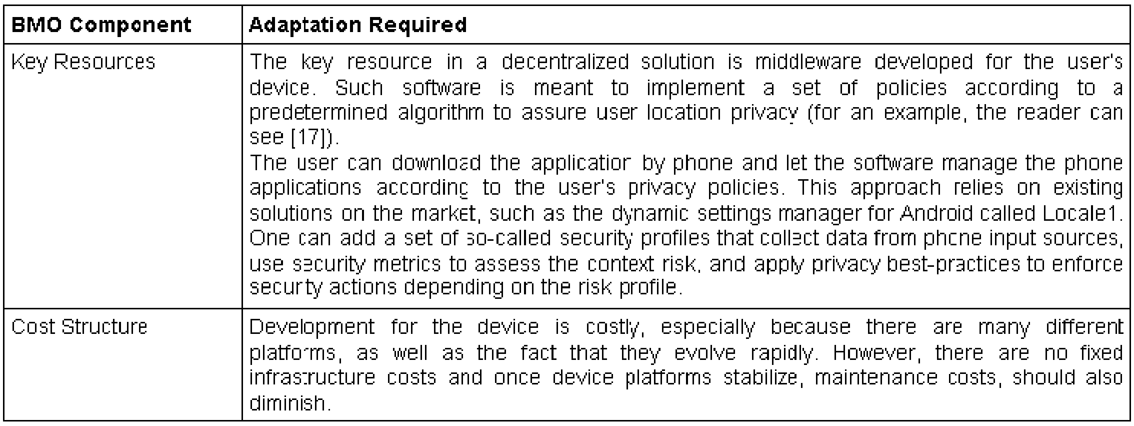
Figure 9.17 shows the business model adaptations for the privacy manager software. Operating system providers of mobile devices such as Orange Telecom are in a good position



BMO Component	Adaptation Required
Key Resources	The platform is composed of a broad range of components between mobile applications, middleware, and server-based software, depending on the technologies chosen to implement the privacy protection (for an example the reader can see [23]).
Cost Structure	The cost of developing the platform. Costs relative to the infrastructure and its maintenance, which can be especially high in the case in which it has to scale for enormous demands for real-time transactions.
Revenue Streams	A fee over secure transactions paid by risk-averse users.

Figure 9.16: Adaptations required for the privacy broker

to influence privacy protection on their platforms. They have direct access to the raw sensor of the phone and can define what information is exposed to applications through their Application Programming Interfaces (API). Moreover, they have the possibility to integrate the privacy middleware directly into the operating system and thereby target the whole market at once. In addition, they might have an easier job integrating a user friendly profile management into the system. Providing a privacy system can further help to expand the dominance of their operating system market share.



BMO Component	Adaptation Required
Key Resources	The key resource in a decentralized solution is middleware developed for the user's device. Such software is meant to implement a set of policies according to a predetermined algorithm to assure user location privacy (for an example, the reader can see [17]). The user can download the application by phone and let the software manage the phone applications according to the user's privacy policies. This approach relies on existing solutions on the market, such as the dynamic settings manager for Android called Locale1. One can add a set of so-called security profiles that collect data from phone input sources, use security metrics to assess the context risk, and apply privacy best-practices to enforce security actions depending on the risk profile.
Cost Structure	Development for the device is costly, especially because there are many different platforms, as well as the fact that they evolve rapidly. However, there are no fixed infrastructure costs and once device platforms stabilize, maintenance costs, should also diminish.

Figure 9.17: Adaptations required for the privacy management software

9.6.3 Can we combine privacy broker and privacy manager software?

Google appears to be an ideal candidate for becoming a centralized service for managing user privacy profile. Google already offers single sign on user authentication and has a mobile phone operating system (Android), which includes location applications (Latitude). Consumers use Google to handle private information like emails (Gmail) and documents (Google Docs). In addition, the company has already implemented some aspects of an infomediary with the Google health offering, as well as a dashboard which gives users an overview of all available services and settings.

Google is in a special position where it can choose to implement either a privacy broker model around the server infrastructure or integrate a privacy manager into the Android operating system. This gives the company the unique opportunity to also choose a mix of both alternatives. The solution could be more independent (phone based middleware) or when deliver real-time centralized server based privacy mediation.

The caveat is that Google is a private company and the main business model is to sell targeted advertising, which might conflict with privacy protection ideals.

9.6.4 Privacy market

In a privacy market, the customer can sell his, her, or its personal data. A practical case of a privacy market is Allow Litd [8]. This London-based firm takes advantage of a recent English regulation that obliges a company to erase all users' data collected without their consent. Once a client signs in with Allow Ltd, the company scans all firms' databases looking for the client's personal data. Once the personal data are found, the firms are requested to remove those data unless they pay a small price, 70% of which goes to the client.

This type of service provider supports the management of the user's sale of the property right over data. For this kind of task, the use of a privacy mirror (as those illustrated by [167]) seems to be appropriate.

Facebook appears to be a good candidate for the privacy market. In the last five years its privacy policy has increased from 1000 words to some 5900 words. We intend this effort as an attempt to get consent over user's partial loss control of property right over the data (Facebook uses non-exclusive license of the user's data). The user therefore looses the control over personal data in exchange of some services. No additional software is required to access Facebook and the architecture used to assure user's privacy is fairly standard.

9.7 Discussions and conclusions

In this paper we introduced the business model of a trusted third party to protect privacy while enabling location based services. We ground our claims on a model developed specifically by incorporating existing works. The empirical data we collected extended previous knowledge in privacy management. We referred to business model ontology to derive a set of guidelines for business model designers and identified possible variations to our pattern of the privacy friendly business model inspired by the infomediary business model. We presented some market players who are potential candidates to provide instantiations of such a privacy protection service.

According to our findings we answer our research questions by addressing three sub-questions as follows:

R1: What is the specificity of privacy management in the location-based mobile B2C market?

Our empirical evidence in section 4 strongly suggests that collected data reduces user payoff, whereas the combination of service personalization and data control increases user payoff. We confirm previous evidence [179] of a relation between service personalization and user payoff, and extend it with the notion of control in the B2C market. We also found two clusters which behave slightly differently than what has been seen for Internet privacy [138]. Our model is both simple (4 constructs) and representative (adj R2 between 0.22 and 0.45).

R2: Which business model components allow a high level of mobile user payoff, while keeping the collected data to a minimum?

We suggest that business model designers should follow the infomediary pattern and then define the degree of software centralization according to how much data should be collected and how much control should be left to the user. According to the type of firm involved, a privacy broker and a privacy manager software or both is to be preferred.

R3: How should the differences in payoff among privacy risk neutral and privacy risk adverse mobile users be addressed?

Although both customer segments care about the personal data they disclose, privacy risk neutral mobile users seem to be more attentive to a combination of data control and service personalization in exchange for their data. The privacy risk adverse users obsesses about the data and therefore a pay-per-use Single-Sign On service that safely protects their data and acts as a proxy to other services seems more likely to be profitable.

Our proposed model is to be considered as an initial step to conceive a tool to support strategic decisions and it has its own limitations. Concerning the evaluation of the model, the business model guidelines have been instantiated, but their impact on firm performance has not been empirically tested. On a more general level we assume privacy will become a technological trend. Privacy has gained awareness only in the last years and its growth is yet to come. The definition of privacy guidelines within a common framework has just started and there are no largely adopted solutions integrated by platforms. As long as there is no standard and no real added value or perceived added value to enforce privacy, there is always the possibility to go directly to the vendor and use raw data from the phone sensors.

We feel that this paper offers some interesting [66] contributions to the field:

- We defend the view of those who believe that privacy should not be seen only as a cost. We propose and show evidence that it could be a value proposition of a business model in the B2C mobile market to complement product customization and risk reduction.
- We suggest that secure service personalization for customer and data access for the company can co-exist sustainably (by means of a third party - to be tested later).
- We present more than one way an enterprise can position itself in relation to its competitors in relation to the trade-off between data control and service personalization. We argue by a set of instantiations that the mobile platform can play a key role at multiple levels (OS, device manufacturer, and operator) in the implementation of these new business models.

Supposing that no third-party actor emerges, some firms might implement some elements from our proposed pattern to add privacy risk mitigation in their value proposition and gain new customers. In the long term this kind of firm would no longer require a third-party actor.

Accordingly, one could decide to remove our initial assumption regarding the existence of a third party actor. In that case the best strategy for a firm is to internalize the third party, if it involves its core competences. This again might raise strategic issues about service integration and business model unbundling.

Further work should address issues such as the possibility of leveraging our proposed privacy business model pattern in other economic contexts, involving incomplete agreements and lack of trust amongst involved parties.

Chapter 10

Analysis of serious games implementation for project management courses

Abstract

Previous researches in pedagogy and project management have already underlined the positive contribution of serious games on project management courses. However, the empirical outcome of their studies has not been translated yet into functional and technical specifications for serious games designers. Our study aims at obtaining a set of technical and functional design guidelines for serious game scenario editors to be used in large classes of project management students. We have conceived a framework to assess the influence of different serious games components over student's perceived acquired competency. Such frameworks will allow us to develop a software module for reflective learning, which is meant to extend theory of serious games design.

10.1 Introduction

Information system (IS) project management courses are known to be challenging to conceive, since most of the skills required for project managers cannot be achieved ex cathedra. Problems in IS are characterized by incomplete, contradictory and changing requirements, and solutions are often difficult to recognize because of complex interdependencies. This leads to an educational dilemma in teaching such problems because a rich background of knowledge and intuition are needed for effective problem-solving. Hence complexity is added rather than reduced with increased understanding of the problem [54].

As a consequence of the large number of failed projects a strong challenge to traditional methods of project management based on universal best practices (such as the Project Management Institute) emerges in the academic world and among practitioners [110, 211]. Traditional approaches are part of a very instrumental and functionalist vision of promoting project management principles that do not reflect the reality of the projects, which is ambiguous, fragmented, complex, socio-technical built, and with a strong political character. Therefore, project management is a discipline that requires knowledge and reflective practice that allows players to lead the project team in an emergent way. This kind of frameworks requires a high degree of interaction between teacher and students. But face-to-face exchanges are hard to manage when the number of students is greater than forty [225].

Game-based learning (also known as serious games) uses simulation to allow students to actively acquire competences required to solve problems. Hence game-based learning scenarios might be the solution to introduce large classes to IS project management since they are known to have an effect on student's self-efficacy as well as acquisition and retention of declarative and procedural knowledge [223]. Yet little interest has been given so far on how to design a scenario editor to support an IS project management course by means of game-based learning. In software engineering courses, game-based simulations are far less used than other types of educational approaches (e.g. industrial partnership or team learning) and they lack to incorporate model-based instruction and reflective learning [165]. We expect a similar trend in IS project management courses.

Therefore our research question is: How to design a game-based learning scenario editor to support an information system project management course for more than forty students?

By adopting a design science methodology this study aims at obtaining a framework to design game-based learning scenario editors to enhances project management competences for students attending the course. Such framework is induced by testing different software components to assess their influences of students' acquired competency. Therefore the creation of a model to assess the software components described in this paper is the initial step of such study. We start here by assessing the gaps in the existing literature and by deriving a conceptual model in the next section. The third section illustrates the methodology we adopt to test our conceptual model and to assess the pedagogical effect of different software tools. The results of a first assessment performed in one of these teaching courses are presented in the fourth section as example. The paper ends by discussing the results obtained and by highlighting the next steps of our study.

10.2 Literature review

This section briefly assesses the state of the art in game-based learning for project management course. We are looking for concrete evidences regarding the link between game-based learning and performance of the IS project management course. Hence we use the guidelines of Okoli and Schabram [173] for a protocol to assess the existing literature. For sake of simplicity we decide to limit our Google Scholar search to articles published in the period 2005 -2010. Using the selected keywords (project management; information systems; game-based learning) we obtain 59 results, among which 21 are cited by at least another paper and accessible to us. Since we are interested in articles that have assessed the performance of the serious game analysed, we skim our set of articles to only a few. For those papers we perform forward and backward analysis, i.e. we assess the papers that cite/are cited by them. At the end we obtain two streams of research: ex-ante evaluation and ex-post evaluation. Since we wish to connect these two stream of research we derive three concepts: the student's perceived acquired competency (1), which is the set of measured capabilities that the student acquires in class; the perception of the serious game design (2), which we consider here as the set of features that the game-based learning software possesses to empower the teacher; the student's engagement (3), i.e. the student's will to take part actively to the game-based learning experience.

The first stream of research focuses on the ex ante evaluation of the effect that serious game design has on student's perceived acquired competency. This group of papers claims that while traditional methods are based on an instructivist methodology, game-based learning provides a constructivist learning environment where learners can practice the formulation of requirements specification through requirements elicitation and learning by doing [103]. In addition to that game-based learning provides a challenging and complex real-world environment within which to apply their theoretical knowledge to overcome difficulties in dealing with ambiguity and vagueness, while developing self-confidence and increased motivation [67].

The second stream of research focuses on the ex post evaluation of the effect that student's engagement having played the serious game has on the student's perceived acquired competency. Researchers collect student's suggestions for game changes [183, 61] and perceived competences needed [183, 97, 260].

To link these two streams of research we suggest considering the student's engagement as a mediator between serious game design and student's perceived acquired competency. At the end we derive the following set of hypotheses:

(H1) the perception of the serious game design influence the student's perceived acquired competency; (H2) the student's engagement influences the student's perceived acquired competency; (H3) the perception of the serious game design influences the student's engagement. In the next section we illustrate how we intend to design an experiment to test our hypotheses.

10.3 Methodology

In this section we briefly describe the methodology we use to perform our experiment. Design science seeks for outcomes that can be relevant for practitioners and that have been obtained in a rigorous way. The purpose in this kind of study is usefulness rather than truth. Although design science has been used since many decades, it has been officially accepted in information system since the Management Information System Quarterly article of Hevner et al. [109]. In our study and in this paper we adopt the methodology suggested by Peffers et al. [182], which proposes a process composed of six steps. Following the first step we clearly identify our problem, using the literature review, as summarized by our research question.

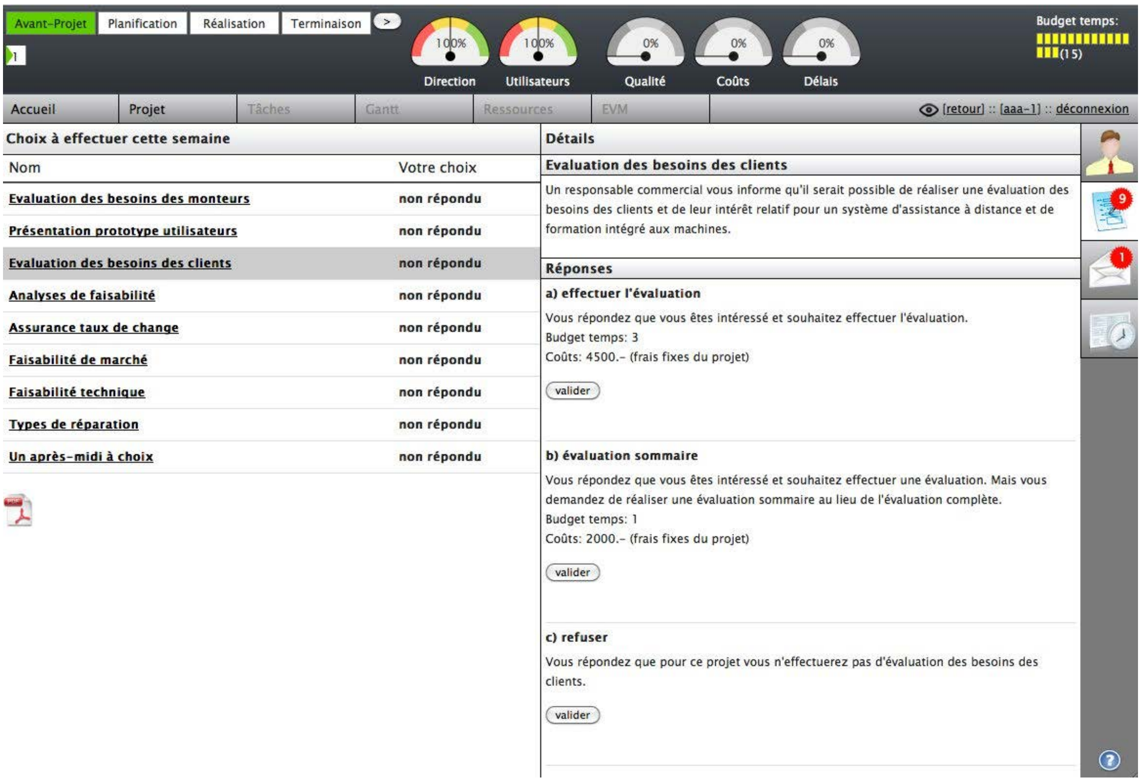
The second step of the methodology identifies the objectives of the solution. In this sense, in the previous section we have identified two gaps in the literature: the first one concerns the link among ex ante and ex post evaluation criteria, whereas the second one regards the use of reflective learning by means of serious games. Thus our study should start by conceiving a framework to assess the correlation among ex ante and ex post evaluation criteria. Then we will move towards the development of an additional module for reflective learning over the student's achieved skills and towards the assessment of its added value.

10.3.1 Design and development

In the third step of the methodology the design and development of the new component occurs. Yet in the first part of our study described here, the development is minimal since we have decided to reuse an existing serious game. The selected platform to test our assessment framework is a game-based learning scenario editor called Albasim. The main reason underlying the choice of such platform is its large set of existing features and the direct link that the authors have with the development team of the software. This is going to be very useful during the second part of the study, when we will be developing an additional component. Figure 10.1 illustrates the dashboard used by the game players by means of a web browser. On the top right corner there are the key performance indicators. On the top left corner of the screen the four stages of the game are illustrated: the players start by the project initiation (1), then they move on by planning the project (2) and executing it (3) before closing it (4). The central part of the screen is multifunctional, whereas the right side of the central screen allows the player to manage resources and task, and to read e-mails send by the central system. For what concerns the reflective learning, the system does not have a dedicated feature, leaving to the teachers the task to arrange students' presentations to share lessons learned, as explained in the following section.

10.3.2 The pedagogical scenario implemented

The fourth step of the methodology of Peffers et al. [182] requires a demonstration of the artefact. In our case the game requires two four-hour sessions, for a total of eight class hours over two weeks. Before the first session the students receive the software manual and the business case. At the beginning of the first session students get familiar with the idea of serious game and to the functionalities of the software (e.g. the dashboard). Then the students are asked to gather in group and to collect and process information own by the different fictive players in the game, in order to deliver a project proposal to be validated with the client (i.e. the professor). During the rest of the week the students are supposed to work in group to complete the assignment and send the improved project proposal to the professor, who choses two proposals among them. At the beginning of the second game session the chosen grooups are asked to do a short presentation of their project proposal to the rest of the class. Once two student groups have presented the teachers gives them a constructive feedback and add some remarks about the overall performance of the other groups (best and worst practices). After the presentations the teacher recalls to the class key theoretical concepts regarding project planning. Then the students are asked to work in group to make and to justify their planning decisions, while taking into account a set of constraints (time, cost, quality, resources availability and risks). In the rest of the week student groups are ask to finalize the WorkBreakdown Structure, Program Evaluation and Review Technique and Gantt diagrams, together with cost estimations.



Choix à effectuer cette semaine

Nom	Votre choix
Evaluation des besoins des monteurs	non répondu
Présentation prototype utilisateurs	non répondu
Evaluation des besoins des clients	non répondu
Analyses de faisabilité	non répondu
Assurance taux de change	non répondu
Faisabilité de marché	non répondu
Faisabilité technique	non répondu
Types de réparation	non répondu
Un après-midi à choix	non répondu

Détails

Evaluation des besoins des clients

Un responsable commercial vous informe qu'il serait possible de réaliser une évaluation des besoins des clients et de leur intérêt relatif pour un système d'assistance à distance et de formation intégré aux machines.

Réponses

a) effectuer l'évaluation

Vous répondez que vous êtes intéressé et souhaitez effectuer l'évaluation.
Budget temps: 3
Coûts: 4500.– (frais fixes du projet)

b) évaluation sommaire

Vous répondez que vous êtes intéressé et souhaitez effectuer une évaluation. Mais vous demandez de réaliser une évaluation sommaire au lieu de l'évaluation complète.
Budget temps: 1
Coûts: 2000.– (frais fixes du projet)

c) refuser

Vous répondez que pour ce projet vous n'effectuerez pas d'évaluation des besoins des clients.

Figure 10.1: Dashboard of Albasim (Source: www.albasim.com)

10.3.3 Evaluation

The fifth step of the methodology concerns the evaluation of the artifact. To operationalize our constructs we reuse existing items from the two streams of literature whenver possible and we obtain a set of five-point Likert scale items, which are meant to be collected by questionnaire to be handed once the students have completed the assignments of the second game session. For the student's perceived acquired competency we derive four items inspired by Zapata [260] and Mawdesley et al. [153]. For the serious game design we implement seven items inspired by Hainey and Connolly [103] and de Freita and Oliver [67]. For the student's engagement we use seven items inspired by Gresse von Wangenheim et al. [97] and Dantas et al.[61]. A set of open questions has been collected as well, but their answers will be not presented here for sake of brevity.

10.4 Current results

We have tested the serious game with a sample of bachelor students enrolled in a project management course with a special focus on information systems. We have collected students' perception by means of an electronic survey. We have obtained 74 answers out of the total of 104 students. Although limited in size, we consider this sample as representative for our study and a good starting point to perform statistical analysis using Stata 11. We started by performing the Cronbach's alpha test over each set of items to measure how well each set of items was representing the concepts. A Cronbach's alpha value of 1.00 would be optimal, whereas a value below 0.70 should be rejected. In our case we obtained the following results: acquired competency = 0.79; design = 0.80; engagement = 0.77.

While testing the causality effect we have performed seemingly unrelated re-gressions among the three constructs obtained by performing the average of each set of items (i.e tau-equivalent factor loadings). In other words we have asked Stata 11 to tests all the regressions at once.

Figure 10.2 represents the results that we obtained and it shows that serious game design has also a direct effect over student's acquired competencies, which is statistically significant (p¡0.01). It also appears that the student's engagement has an effect over the student's perceived acquired competency that is statistically significant (p ¡0.05). Finally the serious game design has an effect over the student's engagement that is statistically significant (p ¡0.01). Thus all hypotheses are confirmed.

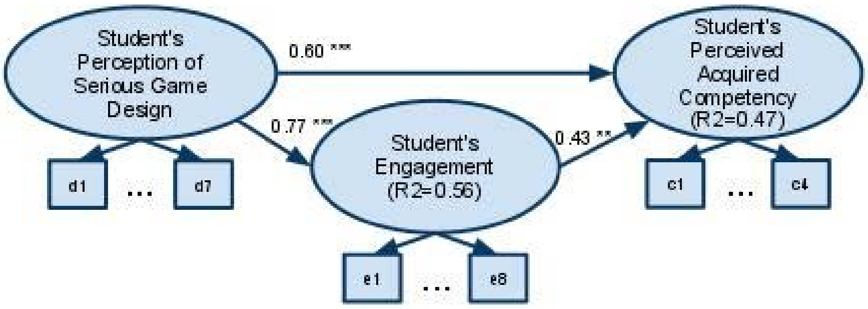

Student's Perception of Serious Game Design
0.60 ***
Student's Perceived Acquired Competency (R2=0.47)
0.77 ***
Student's Engagement (R2=0.56)
0.43 **
d1
...
d7
e1
...
e8
c1
...
c4

Figure 10.2: Results of the preliminary test

The direct and indirect effect of serious game design explains almost 50% of student's perceived acquired competency variance among students (R2=0.47). This is to say that none of the two effects should be neglected. In addition to that the student's engagement variability among students is largely explained by serious game design (R2=0.56), which leads us to believe this model has a good explanatory power. We have also controlled for the effect of sex and nationality and the results were not statistically relevant.

10.5 Conclusions and further works

We start this section by recalling our research question: How to design a game-based learning scenario editor to support an information system project management course for more than forty students? In this paper we present our framework to link ex ante and ex post evaluation criteria to assess a game-based learning editor. Now that the framework is in place we can develop the reflective learning module and we can assess its added value by using such module on a subset of the overall students' sample, treating the rest of the class as control group. The results we obtained so far lead us to believe that serious game design has a direct and indirect effect over student's perceived acquired competency, which is mediated by student's engagement. The module we wish to develop has a graphical interface that allows the scenario designer to represent the scenario as a graph. The module is expected to be able to mine the log of student groups' actions and to represent them under the shape of graphs, in order to benchmark the different groups' experience.

In the next iteration we intend to have students groups playing different versions of the same game, whereas the student's acquired competency will be tested with a set of questions in the final exam of the course. These improvements should increase the reliability of our results against endogeneity due to common method variance [9].

Chapter 11

From "Security for Privacy" to "Privacy for Security."

Abstract

This article envisions the use of context-awareness to improve single sign-on solutions (SSO) for mobile users. The attribute-based SSO is expected to increase users' perceived ease of use of the system and service providers' authentication security of the application. From these two features we derive two value propositions for a new business model for mobile platforms. The business model can be considered as an instantiation of the privacy-friendly business model pattern presented in our previous work, reinforcing our claim that privacy-friendly value propositions are possible and can be used to obtain a competitive advantage.

11.1 Problem Identification

This paper assesses ways for context-aware mobile applications to authenticate a mobile user using Personal Identifiable Information (PII). According to previous literature, information security is required to protect PII and ensure users' privacy; yet such security implies a trade-off between the system developers' effort to implement privacy-enabling technologies and the cognitive effort required by the user to use such technologies. Consider a mobile user trying to access a set of web services, as shown in the top part of 11.1. The user has to pass a set of access controls for authentication, identification, authorization, and accountability. This security procedure increases the user's perceived performance of the protection application, but it negatively affects the ease of use of the system. Previous studies [118] have shown how low perception of ease of use can lead to lack of user compliance with security policies. A single sign-on (SSO) solution can increase the ease of use, as shown in the middle part of figure 11.1. Solutions like Firefox's built-in password manager increase ease of use but reduce the amount of effort attacker must put forth to access the user accounts since there is only the master password to break. In order to offer stronger authentication SSO usually requires a shift from an access control list system (e.g., passwords) to a capability-based system (e.g., biometric controls or multi-factor authentication). However this approach lack of flexibility, since users biometry cannot be changed over time. We believe that context awareness can help us to achieve the proper trade-off between dynamic authentication and ease of use, as shown in the bottom part of 11.1.

Since the early 1990s, context-aware mobile computing has received interest from scholars [69][213]. For the purposes of this paper, we refer to context as *any information that can be used to characterize the situation of [...] a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves*[69]. Based on this definition, there are four types of primary context: *location*, *identity*, *activity*, and *time*. These types characterize a situation by answering where, who, what, and when, respectively. We are looking for a system that can transparently authenticate the user and dynamically adapt to the user's behavior. Therefore, our research question is: **How can context-awareness be used to improve authentication security and ease of use, while designing SSO applications for mobile devices?**

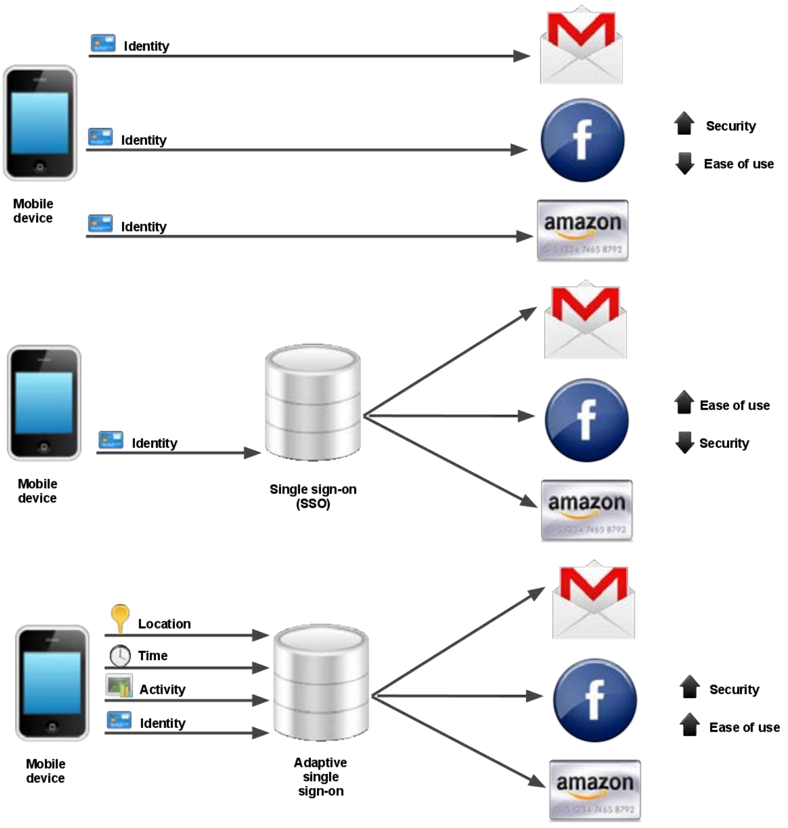


Figure 11.1: Adaptative Single Sign-On (ASSO) for security and ease of use

In the rest of the paper we adopt the methodology proposed by Peffers et al. [182]. The next section presents an illustrative scenario to introduce the solution we aim to achieve.

The third section lists the objectives of our research, and the fourth section illustrates a set of business model considerations concerning the application of our solution. The last section concludes by listing the contributions of this paper and the research directions it opens.

11.2 A Simple Illustrative Scenario

Figure 11.2 represents a simple scenario presenting the adaptive single sign-on solution.

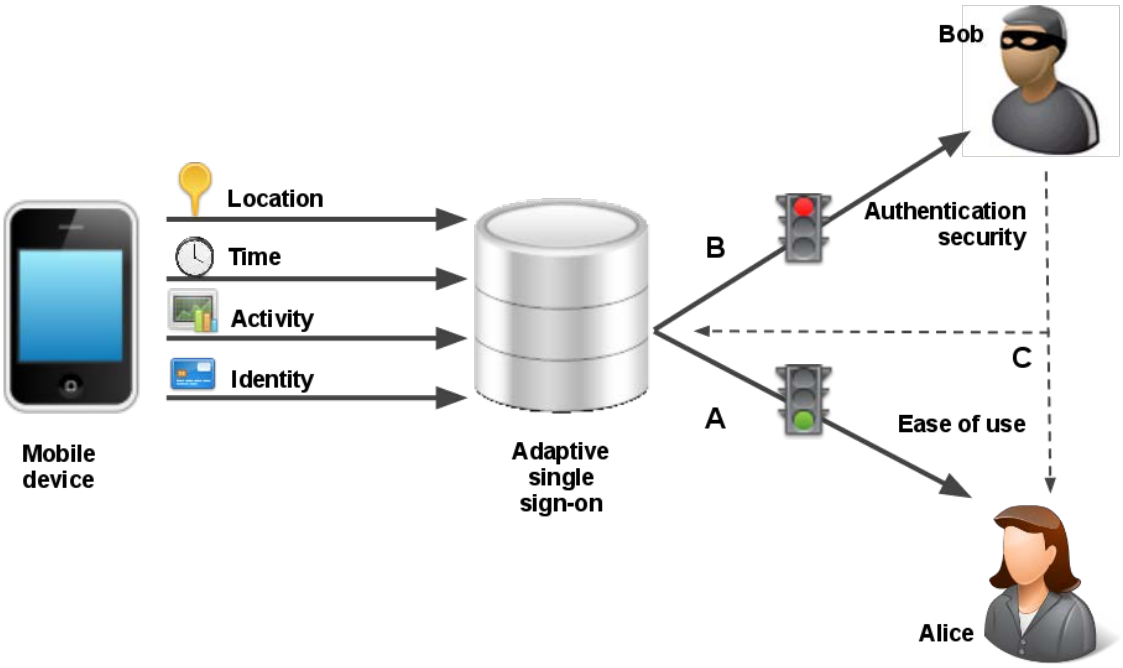


Figure 11.2: Process of ASSO solution for a context-aware mobile device

11.2.1 Alice accesses her Internet accounts

The end user, Alice, has a mobile device with a paid application called *Privacy Manager*. This application uses adaptative authentication to combine real-time transaction data with Alice's behavioral profile. Real-time transaction data used to identify Alice include her current location, speed (activity), and time. Once the data analysis application returns a positive authentication result, Alice can check her e-mail and bank accounts online through the protected channel. Thanks to *Privacy Manager* she can access her email and bank accounts without having to enter any passwords, as long as data analysis returns a positive result.

11.2.2 Bob cannot access Alice's accounts

Assume that a thief (Bob) plans to steal Alice's mobile device to access Alice's bank account. Once Bob steals the device, the real-time transaction data does not match the data stored in Alice's profile. Suppose Bob knows this authentication method, and he tries to to follow Alice before stealing the phone: Bob would note her location at any given time and collect personal information about Alice in order to copy her behavior. However the *Privacy Manager* applies state-of-the-art obfuscation techniques to not disclose any information about the activity and the identity of Alice, leaving Bob with only half of the information required.

11.2.3 Alice goes on holiday

When Alice goes to another city to see a friend, *Privacy Manager* detects that the behavior disclosed does not match Alice's older profiles. Neverless Alice possesses a trusted mean of identification (e.g. a password) to provide user's identification. After identification, *Privacy Manager* creates a new profile and stores data to include Alice's behavior on this day. When Alice comes to this city again to see her friend, her behavior data will be matched with this profile.

11.3 Objectives of the Solution

From a cognitive point of view, usability issues arise when users cannot properly manage the information required to sign in to different web services using a large set of different pseudonyms and passwords. The possibility of capturing the change in the identity of the real user (the features of his or her everyday life behavior) has been considered only as a threat to his or her privacy. We propose to shift from a discretionary access control approach to an attribute-based approach, where the attributes are features of the user's environment and his or her behavior in that context.

This approach provides a high level of control over access to the services while maintaining its high level of usability for mobile users, under the assumption that each user has a unique pattern of behavior. In previous studies, context-aware technology has evoked concerns about privacy. Location-based applications track users automatically on an ongoing basis, generating an enormous amount of potentially sensitive information so the identity of the owner of the mobile device can be implicitly obtained from the analysis of its location [20][81]. However, we see great potential in this potential threat, and we formulate our starting assumption in the form of a null hypothesis: **context is a unique user identifier (H0)**.

Context-based authentication is currently used for credit card fraud detection relying primarily on artificial intelligence techniques using unsupervised learning methods [22]. Machine learning usually refers to evolved behaviors based on empirical data, such as that from sensor data or databases associated with artificial intelligence. The information is acquired during authentication through a learning process to authenticate the mobile user.

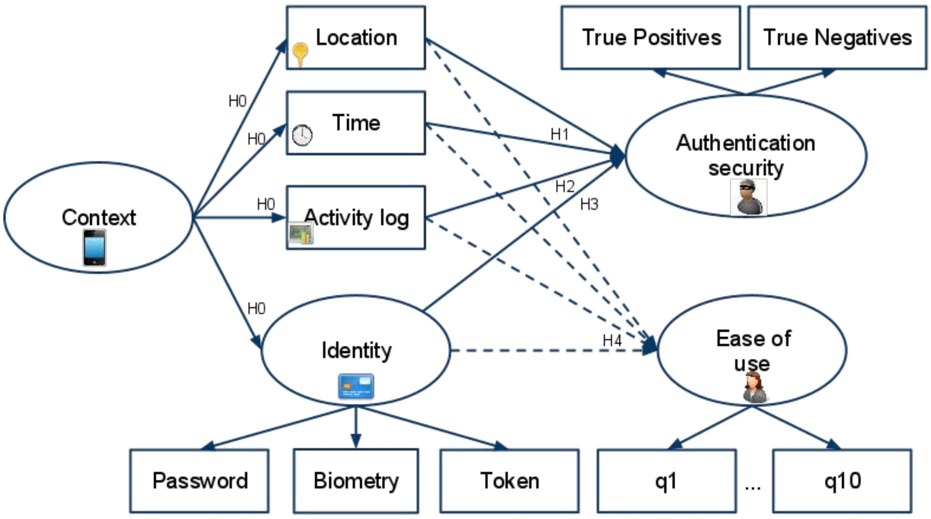


Figure 11.3: Theoretical Model

The asserted advantages of machine learning are accuracy comparable to that achieved by human experts and considerable savings in terms of expert labor power, since no intervention from either knowledge engineers or domain experts is needed for the construction of the classifier or for its porting to a different set of categories [214]. User data clustering can be performed on two levels: on one hand, the best matches and the corresponding data points can be automatically or manually grouped into several clusters so outliers can be easily detected, and the alert will be activated once the number of outliers exceeds the predefined threshold. On the other hand, new trends can be found when regions on the map representing a cluster are identified and used for classification of new data. To test our hypotheses we propose a system that collects a set of mobile sensor data and compares them to a known set of user's profile. Moreover we suggest using an escalating procedure to minimize the computational effort of the system for most authentication cases. Therefore a limited amount of phone sensor data are collected by the context-awareness component, and through the machine leaning the mobile phone can determine whether it is dealing with an authorized user or not. If the result is positive, the user is authorized to access the services (e.g., Amazon, Gmail, Facebook); otherwise, additional contextual information (escalating from time and location up to activity and, eventually, identity) about the user is collected and analyzed before access to any service is granted. 11.3 presents the structural model. A rectangular element is associated with a variable that can be directly measured, whereas an oval represents a latent concept that has to be measured indirectly by summing the variables to which it is associated.

We define authentication security as the number of true positives and true negatives obtained by the system. In other words, we aim to minimize the number of occurrences in which the user is not allowed to access the system (false negative) or an unauthorized person is allowed to access the system (false positive). We have already stated that location data can be used to infer much about a person, even without the user's name attached to the data [133]. In our case, let us suppose that the user goes to work every day and comes back following the same routine. In this case, the system would assess the user's location at a certain frequency against the expected pattern (home-work-home). Thus, we derive our first hypothesis: **the conjoint effect of time and location increases authentication security (H1).**

There may be cases when the home-work-home pattern lacks sufficient variance to discriminate the user from other people. For example, someone physically close to the user could take the phone while it is unattended and access a number of services. Since the phone does not change location, the unauthorized access would be possible, even if for a limited amount of time. To address this problem, the system detects when the variance among the collected data is too small, and in that case collects the user's activities (e.g., web pages visited) against known activity patterns. Previous research has shown that such activity patterns are also discriminant [12]. Thus, we derive our second hypothesis: **the conjoint effect of time, location, and activity increases authentication security (H2).**

Many users do not often follow repetitive patterns. For this reason, the fourth contextual dimension (i.e., identity) is used when sensor data do not fall into any known pattern. To update the behavioral patterns we grant access rights to the user after proper identification (e.g., by means of a password, biometric control, or near-field communication card). This kind of identification has already been used by a large set of services. Banks call credit card users after an unexpected buying pattern, and Facebook asks for the answer to a secret question when the user tries to access it from a foreign country. Thus, our third hypothesis arises: **the conjoint effect of time, location, activity, and identity increases authentication security (H3).**

A final consideration concerns how we handle ease of use, which we measure using Venkatesh's [243] survey items (indicated in 11.3 as q1-q10). We believe that our escalating approach, combined with the machine learning techniques for classification and the eventual use of available solutions for identification would reduce the number of human-computer interactions required for authentication, increasing the user's perceived ease of use. This idea is in line with similar research currently undertaken by banks to obtain mobile-payment devices that do not use passwords [228]. Thus, we derive the last hypothesis: **the conjoint effect of time, location, activity, and identity increases ease of use (H4).**

11.4 The Business Model

This section extends the business model pattern to a third party in charge of managing the privacy of mobile users, third-party and mobile services providers [145]. For the sake of coherence with the approach previously used we apply the business model ontology (BMO) of Ostewalder and Pigneur [175]. This approach allows us to represent a business model, whose value propositions are derived from the two performance criteria of our theoretical model (i.e. ease of use and authentication security). The following paragraphs use the nine business model elements defined by BMO to assess the strategic contribution of our adaptive single sign on (ASSO) application for context-aware mobile device.

Value proposition: it is at the center of the business model. It describes which customer problems are solved and why the offer is more valuable than similar products or services from competitors. The privacy-friendly business model pattern presented in [145] had four value propositions. One value proposition (personalized) that concerned the privacy risk-neutral customer segment is out of scope since it concerns distributive justice. Another (matchmaking) that concerned the typical added value of a third party is not changed. The two remaining value propositions (privacy risk mitigation and customer data analysis) do not change, but their corresponding customer segment is inverted. Therefore, customer data analysis for ease of use is associated with the mobile user instead of with the service provider. Our context-aware ASSO solution increases the level of usability without sacrificing its protection level. At the same time, the mobile device authenticates the mobile user through an accurate learning process that has no other costs. Risk mitigation by means of security authentication is now associated with service providers instead of mobile customers

Customer segments: In the BMO customers are analyzed and separated into groups to help identify their needs, desires, and ambitions (singles, families). In our new pattern, we pass from four to two distinct customer segments: the mobile user seeking ease of use and the service provider seeking authentication security. Since our solution can benefit both mobile users and service provides, our business model patterns is similar to an infomediary between two customer segments.

Customer relationship: it specifies what type of relationship the customer expects and how it is establish and maintained (promotion, support, individual, or mass). Since we do not introduce any significant change for this business model component, the key to attracting users is to promote the importance of privacy protection and to build a strong trust relationship with the customer. We define trust as *a willingness to rely on an exchange partner in whom one has confidence* [159]. A trust relationship may be built on physical, social, economic, or emotional characteristics.

Channel: it illustrates how the customer wants to be reached and by whom the customer is addressed (e.g., the Internet, a store). We do not introduce any significant change to this business model component. Our ASSO application for a context-aware mobile device is based on the mobile phone for an end user. The authentication technology would be provided under the shape of a service providing an application programming interface (API) or an application made with a software development kit (SDK).

Key activities: they are used to transform all resources into the final product or service (development, production, proprietary process). In the new pattern, we maintain the previous key activities (control and build network), and we introduce the important concept of adaptative authentication, which implies unsupervised rule generation. The user can be authenticated by identifying the feature of the user's behavior pattern through machine learning, but if the context-based authentication fails, an adaptive authentication is required.

Key resources: staff, machines, and proprietary knowledge are required to deliver the value proposition. In the new pattern, we maintain the previous key resources (user data, brand, and platform access) and eventually add the algorithm for adaptative authentication.

Key Partners: for resources or activities, most businesses depend on an external partner network (logistics, financial) that which can provide better quality or a lower price on non-essential components, and we introduce no significant changes for this business model component. In order to guarantee the trust worthiness and security of this solution and to be able to certify that application made for this platform is compliant our solution has to be certified by an external certification provider. To offer additional services, our solution must also be in relationship with a mobile user and a service provider.

Revenue streams: they reflect the value the customers are willing to pay and how they will perform the transaction. In the new pattern, the two revenue streams associated with the two selected customer segments are switched: the end user pays a fee to use the application, and the service provider pays a fee for each secure transaction (or it could by a license to develop a set of ASSO applications).

Cost structure: it is another side of financial information and it should be aligned to the core ideas of the business model. In the new pattern, we maintain the previous key resources (network building, platform management, and development) and eventually add the dynamic authentication algorithm management.

11.5 Discussions and Conclusions

This paper proposes a new instantiation of the business model pattern presented last year at BMMP 2010[23] and described in detail in a journal article [145]. Our new model has privacy at the core of its value proposition whereas previous instantiations considered privacy as a complementary service to be aggragated to other value propositions.

Therefore this paper makes three contributions: (1) we present an improved solution for SSO using the mobile user’s attributes; (2) we reinforce our previous call for better and more privacy-friendly business models; and (3) we present new ways to use privacy as key component of mobile business models.

In the current stage of project development, we acknowledge a set of limitations. The first one concerns the choice of the approach to represent the business model. Since we wanted to instantiate an existing business model pattern, we kept the same representation, but we acknowledge the existence of alternative business model frameworks, such as Bouwman et al. [31] and Wegmann [248], that may be more geared to mobile since they can take the mobile or ICT service as a unit of analysis. We also acknowledge that IBM and Vodafone are currently developing a software solution similar to the one proposed here. However, since their solutions are proprietary, we could not include information about their performance.

As future extensions of our solution, we recall the *mobile device vs central server* options presented in the previous work [145] and we intend to explore two *what-if* scenarios, which arise when one of the two agents takes the lead:

(1) *What if the ASSO is owned by services providers in a situation of coopetition?* In this case, the application would mostly reside in central servers of service providers. These providers would use an ASSO API to develop new applications or by defining an ASSO standard. The mobile user would use a client application on the mobile device that would send the context information in order to obtain authentication. This approach would

increase the performance of the authentication algorithm, which could take advantage of power the central server and that could decrease its learning time by having a larger pool of users' data. Moreover the update of client's application would be easier to perform and user's data could reside on the server to not leave anything on the mobile in case of stealth.

(2) *What if a device-centric authentication is preferred to the ASSO platform?* In this case, the ASSO would mostly reside on the user's mobile device. The authenticating algorithm would be stored within a mobile application that would establish a secure connection with the service provider after user's authentication. This approach would address privacy concerns, which might arise against the centralized solution, since in this case the user's data are not stored in the server. Additionally this approach is expected to drain less battery power, since the increased computational effort would be compensated by the reduction of client-server data exchanges required in the first scenario. In a possible extension of this scenario users could authenticate each other without the need for a third party. This solution would spread the user's data among peers, in order to reduce the success chances of malicious attacks [181]

Bibliography

[1] R. L. Ackoff. Management misinformation systems. *Management science*, pages 147–156, 1967.

[2] A. Acquisti, R. Dingledine, and P. Syverson. On the economics of anonymity. *Lecture notes in computer science*, pages 84–102, 2003.

[3] R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann. Taming compliance with Sarbanes-Oxley internal controls using database technology. In *Proceedings of the 22nd international Conference on Data Engineering*, Washington DC, USA, 2006.

[4] AICPA. 70 statement on auditing standards: Reports on the processing of transactions by service organizations. Technical report, 1992.

[5] D. Amyot. Introduction to the user requirements notation: learning by example. *Computer Networks*, 42(3):285–301, 2003.

[6] Chris Anderson. *Free: The Future of a Radical Price.* Hyperion, first edition edition, July 2009.

[7] R. Anderson. Why information security is hard-an economic perspective. pages 358–365, New Orleans, Louisiana, December 2001. IEEE.

[8] Julia Angwin and Emily Steel. Web's hot new commodity: Privacy. *wsj.com*, February 2011.

[9] J. Antonakis, S. Bendahan, P. Jacquart, and R. Lalive. On making causal claims: A review and recommendations. *The Leadership Quarterly*, 21(6):1086–1120, 2010.

[10] Robert Axelrod. *The Evolution of Cooperation: Revised Edition.* Basic Books, New York, NY, USA, revised edition, December 2006.

[11] Ebrahim Bagheri and Ali A. Ghorbani. The analysis and management of Non-Canonical requirement specifications through a belief integration game. *Knowledge and Information Systems*, 22(1):27–64, 2009.

[12] A. L Barabasi. Authors@Google: albert laszlo barabasi, September 2010.

[13] L. Barkhuus. Privacy in location-based services, concern vs. coolness. 2004.

[14] J. B Barney. Firm resources and sustained competitive advantage. *Journal of management*, 17(1):99–120, 1991.

[15] M. Barrett, K. Garrety, and J. Seberry. ICT professionals' perceptions of responsibility for breaches of computer security. 2006.

[16] Scott Beardsley, Luis Enriquez, and Robin Nuttall. Managing regulation in a new era. *The McKinsey Quarterly*, 2009(1):90–97, January 2009.

[17] S. Beer. The viable system model: its provenance, development, methodology and pathology. *Journal of the Operational Research Society*, pages 7–25, 1984.

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

[19] I. Benbasat and R. W. Zmud. The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. *MIS Quarterly*, 27(2):183–194, 2003.

[20] A. R Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46–55, 2003.

[21] Urs W. Birchler and Monika Butler. *Information economics*. Taylor & Francis, 2007.

[22] R. J Bolton and D. J Hand. Statistical fraud detection: A review. *Statistical Science*, 17(3):235–249, 2002.

[23] R. Bonazzi, B. Fritscher, and Y. Pigneur. Business model considerations for privacy protection in a mobile location based context. In *Proceedings of the First Business Models for Mobile Platforms (BMMP) workshop*, Berlin, October 2010.

[24] Riccardo Bonazzi, Charlotte Checcaroli, and Stephanie Missonier. The man behind the curtain. exploring the role of IS strategic consultant. In *6th International Workshop on BUSinness/IT ALignment and Interoperability (BUSITAL 2011)*, London, UK, 2011.

[25] Riccardo Bonazzi, Boris Fritscher, Zhan Liu, and Yves Pigneur. From 'Security for privacy' to 'Privacy for security'. In *Proceedings of the Second International Workshop on Business Models for Mobile Platforms*, Berlin, October 2011.

[26] Riccardo Bonazzi, Arash Golnam, Yves Pigneur, and Alain Wegmann. Respecting the deal: Economically sustainable management of open innovation among co-opeting companies. *International Journal of E-Services and Mobile Applications*, 2012.

[27] Riccardo Bonazzi, Lotfi Hussami, and Yves Pigneur. Compliance management is becoming a major issue in IS design. In *Proceedings of the Italian Chapter of the Association of Information Systems (ItAIS 2008)*, Paris, December 2008. Springer.

[28] Riccardo Bonazzi, Zhan Liu, Simon Garniere, and Yves Pigneur. A dynamic privacy manager for compliance in pervasive computing. IGI Global, 2011.

[29] Riccardo Bonazzi and Yves Pigneur. Compliance management in multi-actor contexts. In *Proceedings of Governance, Risk and Compliance Information Systems workshop*, Amsterdam, June 2009.

[30] J. Bonneau and S. Preibusch. The privacy jungle: On the market for data protection in social networks. *Economics of Information Security and Privacy*, page 121–167, 2010.

[31] Harry Bouwman, Meng Zhengjia, Patrick van der Duin, and Sander Limonard. A business model for IPTV service: a dynamic framework. *info*, 10(3):22–38, 2008.

[32] Adam M. Brandenburger and Barry J. Nalebuff. *Co-Opetition : A Revolution Mindset That Combines Competition and Cooperation : The Game Theory Strategy That's Changing the Game of Business.* Broadway Books, 1 edition, December 1997.

[33] T. D. Breaux and A. I. Anton. Managing ambiguity and traceability in regulatory requirements: A tool-supported frame-based approach. Technical report, North Carolina State University Computer Science, 2007.

[34] BSI. BS 25999-1 business continuity management. code of practice. Technical report, 2006.

[35] BSI. BS 25999-2 specification for business continuity management. Technical report, 2007.

[36] Viktor Bucher and Pierre-Alain Cardinaux. Barometre 2009 des entreprises de taille moyenne. Technical report, Ernst & Young SA, February 2009.

[37] R. J. A. Buhr. Use case maps as architectural entities for complex systems. *Software Engineering, IEEE Transactions on*, 24(12):1131–1155, 2002.

[38] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*, January 2009.

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

[40] French Caldwell. The enterprise governance, risk and compliance platform defined. Technical report, 2008.

[41] French Caldwell. Magic quadrant for enterprise governance, risk and compliance platforms, 2010. Technical report, 2010.

[42] French Caldwell, P.E. Proctor, and M. Nicolett. EMC buys archer for enhanced IT GRC capabilities. Technical report, 2010.

[43] L. Capra, W. Emmerich, and C. Mascolo. CARISMA: context-aware reflective middleware system for mobile applications. *IEEE Transactions on software engineering*, 29(10):929–945, 2003.

[44] Hasan Cavusoglu, Izak Benbasat, and Burcu Bulgurcu. Information security policy compliance: An empirical study of Rationality-Based beliefs and information security awareness. *Management Information Systems Quarterly*, 34(3):523–548, September 2010.

[45] R. K Chellappa and R. G Sin. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2):181–202, 2005.

[46] D. Q Chen. Information systems strategy: Reconceptualization, measurement, and implications. *MIS Quarterly*, 34(2):233–259, 2010.

[47] G. Chen and D. Kotz. A survey of context-aware mobile computing research. Technical report, Citeseer, 2000.

[48] Chin Pang Cheng, Gloria T. Lau, Kincho H. Law, Jiayi Pan, and Albert Jones. Improving access to and understanding of regulations through taxonomies. *Government Information Quarterly*, 26(2):238–245, April 2009.

[49] H. W. Chesbrough. The era of open innovation. *MIT Sloan. Management Review*, 44(3):35–41, 2003.

[50] K. W Chew, P. Shingi, and M. Ahmad. TAM derived construct of perceived customer value and online purchase behavior: An empirical exploration. *Project E-Society: Building Bricks*, pages 215–227, 2009.

[51] A. Colby, L. Kohlberg, and A. Higgins. *The measurement of moral judgment*, volume 1. Cambridge Univ Pr, 2010.

[52] Luca Compagna, Paul El Khoury, Alzbeta Krausova, Fabio Massacci, and Nicola Zannone. How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. *Artificial Intelligence and Law*, 17(1):1–30, March 2009.

[53] United States Congress. The Sarbanes-Oxley act of 2002. http://www.law.uc.edu/CCL/SOact/soact.pdf, 2002.

[54] Thomas Connolly and Mark Stanfield. Using Games-Based eLearning technologies in overcoming difficulties in teaching information systems. *Journal of Information Technology Education*, 5(2006):459–476, 2006.

[55] PriceWaterhouse Coopers. Internal audit report 2012. Technical report, PricewaterhouseCoopers, 2007.

[56] COSO. Enterprise risk management integrated framework- executive summary. Technical report, 2004.

[57] On P Cox, Angela Dalton, and Varun Marupadi. Smokescreen: flexible privacy controls for presence-sharing. *IN MOBISYS*, pages 233—245, 2007.

[58] R. Cox and B. De Jong. The right retained team is critical for successful outsourcing, 2005.

[59] Alex Cullen. Current practices for IT centers of excellence (CoEs). http://www.forrester.com/Role/Research/Workbook/0,9126,47493,00.html, October 2008.

[60] G. Danezis and S. Gurses. A critical review of 10 years of privacy technology. In *Porceedings of "Surveillance Cultures: A Global Surveillance Society?"*, London, UK, 2010.

[61] A. R. Dantas, M. O Barros, and C. M.L Werner. A simulation-based game for project management experiential learning. In *Proccedings of the 2004 International Conference on Software Engineering and Knowledge Engineering*, pages 19–24, Anbert, Canada, 2004.

[62] T. K Das and B. S Teng. A resource-based theory of strategic alliances. *Journal of management*, 26(1):31–61, 2000.

[63] T. K. Das and B. S Teng. Relational risk and its personal correlates in strategic alliances. *Journal of Business and Psychology*, 15(3):449–465, 2001.

[64] T. K. Das and B. S Teng. Trust, control, and risk in strategic alliances: An integrated framework. *Organization Studies*, 22(2):251–283, 2001.

[65] F. D Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 13(3):319–340, 1989.

[66] M. S Davis. That's interesting! towards a phenomenology of sociology and a sociology of phenomenology. *Philosophy of the Social Sciences*, 1(4):309–344, 1971.

[67] S. De Freitas and M. Oliver. How can exploratory learning with games and simulations within the curriculum be most effectively evaluated? *Computers & Education*, 46(3):249–264, 2006.

[68] M. de Reuver and T. Haaker. Designing viable business models for context-aware mobile services. *Telematics and Informatics*, 26(3):240–248, 2009.

[69] H. de Vos, T. Haaker, M. Teerling, and M. Kleijnen. Consumer value of context aware and location based mobile services. In *Bled 2008 Proceedings*, pages 50–62, Austria, June 2008.

[70] D. H. Doty and W. H. Glick. Typologies as a unique form of theory building: Toward improved understanding and modeling. *Academy of Management Review*, 19(2):230–251, 1994.

[71] M. J Dowling, W. D Roering, B. A Carlin, and J. Wisnieski. Multifaceted relationships under coopetition: Description and theory. *Journal of Management Inquiry*, 5(2):155–167, 1996.

[72] Y. L. Doz and G. Hamel. *Alliance advantage: The art of creating value through partnering*. Harvard Business School Press, 1998.

[73] T. Eisenmann, G. Parker, and M. W. Van Alstyne. Strategies for two-sided markets. *Harvard business review*, 84(10):92–101, 2006.

[74] M. El Kharbilii, S. Stein, I. Markovic, and E. Pulvermueller. Towards a framework for semantic business process compliance management. In *Proceedings of the GRCIS'08 Workshop*, Montpellier, France, 2008.

[75] D. S Evans and R. Schmalensee. The industrial organization of markets with two-sided platforms. *NBER working paper*, 2005.

[76] M. Fishbein and I. Ajzen. Belief, attitude, intention and behavior: An introduction to theory and research. 1975.

[77] G. W Flake. *The computational beauty of nature: Computer explorations of fractals, chaos, complex systems, and adaptation*. The MIT Press, 2000.

[78] Organisation for Economic Co-operation and Development. *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing, 2002.

[79] Bank for International Settlements. Basel II: international convergence of capital measurement and capital standards: A revised framework - comprehensive version. http://www.bis.org/publ/bcbs128.htm, 2006.

[80] Python Software Foundation. socket - low-level networking interface - python v2.6.4 documentation. http://docs.python.org/library/socket.html, 2010.

[81] J Freudiger, M.H. Manshaei, J. P Hubaux, and D. C. Parkes. On Non-Cooperative location privacy: A Game-Theoretic analysis. In *Proceedings of the 16th ACM conference on Computer and communications security*, New York, NY, USA, 2009.

[82] Boris Fritscher. Business model designer from sticky note to screen interaction. December 2008.

[83] J. Galaskiewicz. Interorganizational relations. *Annual review of sociology*, pages 281–304, 1985.

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

[85] A. Gangemi. Design patterns for legal ontology construction. In *Trends in Legal Knowledge: The Semantic Web and the Regulation of Electronic Social Systems*. European press academic publishing edition, 2007.

[86] A. Gangemi, A. Prisco, M. T. Sagri, G. Steve, and D. Tiscornia. Some ontological tools to support legal regulatory compliance, with a case study. volume 4. Springer, 2003.

[87] U. Gasser and D. M. Hausermann. E-compliance: Towards a roadmap for effective risk management. 2007.

[88] A. Gericke, H. G Fill, D. Karagiannis, and R. Winter. Situational method engineering for governance, risk and compliance information systems. page 1–12, 2009.

[89] S. Ghanavati, D. Amyot, and L. Peyton. Comparative analysis between document-based and model-based compliance management approaches. In *Requirements Engineering and Law, 2008. RELAW'08.*, pages 35–39, 2008.

[90] G. M Giaglis, P. Kourouthanassis, and A. Tsamakos. Towards a classification framework for mobile location services. *Mobile commerce: technology, theory, and applications*, pages 67–85, 2002.

[91] C. Giblin, S. Muller, and B. Pfitzmann. From regulatory policies to event monitoring rules: Towards model driven compliance automation. *IBM Research Report. Zurich Research Laboratory (October 2006)*, October 2006.

[92] Barney Glaser and Anselm Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction, June 1967.

[93] Arash Golnam, Ron Sanchez, and Alain Wegmann. A systemic approach for modelling and analysis of co-opeting. In *Proceedings of the fourth workshop on coopetition strategy*, Montpellier, France, 2010.

[94] Inc. Google. Google maps API - geocoding. http://code.google.com/apis/maps/documentation/services.html#Geocoding, 2010.

[95] G. Governatori, Z. Milosevic, and S. Sadiq. Compliance checking between business processes and business contracts. In *Proceedings of the 10th IEEE Conference on Enterprise Distributed Object Computing*, 2006.

[96] Shirley Gregor and David Jones. The anatomy of a design theory. *Journal of the Association for Information Systems*, 8(5):312–325, May 2007.

[97] C. Gresse von Wangenheim, M. Thiry, and D. Kochanski. Empirical evaluation of an educational game on software measurement. *Empirical Software Engineering*, 14(4):418–452, 2009.

[98] IT Policy Compliance Group. Annual report: IT governance, risk and compliance - improving business results and mitigating financial risk. Technical report, IT Policy Compliance Group, 2008.

[99] Open Compliance & Ethics Group. Red book 2.0 (GRC capability model). Technical report, 2009.

[100] J. Hagel. Leveraged growth: Expanding sales without sacrificing profits. *Harvard Business Review*, 80:68–79, 2002.

[101] J. Hagel and M. Singer. *Net worth: shaping markets when customers make the rules*. Harvard Business Press, 1999.

[102] J. Hagel 3rd and M. Singer. Unbundling the corporation. *Harvard business review*, 77(2):133, 1999.

[103] T. Hainey and T. M Connolly. Evaluation of a game to teach requirements collection and analysis in software engineering at tertiary education level. *Computers & Education*, 56(1):21–35, 2010.

[104] R. H Hall, J. P Clark, P. C Giordano, P. V Johnson, and M. Van Roekel. Patterns of interorganizational relationships. *Administrative Science Quarterly*, pages 457–474, 1977.

[105] O. Hart and J. Moore. Contracts as reference points. *Quarterly Journal of Economics*, 123(1):1–48, 2008.

[106] J. Heiser and al. Hype cycle for governance, risk and compliance technologies, 2008. Technical report, Gartner, Inc., 2008.

[107] J. C. Henderson and N. Venkatraman. Strategic alignment: Leveraging information technology for transforming organizations. *IBM systems journal*, 32(1):4–16, 1993.

[108] Debra S. Herrmann. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI.* Auerbach Publications, 1 edition, January 2007.

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

[110] D. Hodgson and S. Cicmil. The politics of standards in modern management: Making the project a reality. *Journal of Management Studies*, 44(3):431–450, 2007.

[111] R. Hoekstra, J. Breuker, M. Di Bello, and A. Boer. The LKIF core ontology of basic legal concepts. 2007.

[112] W. Michael Hoffman, John D. Neill, and O. Scott Stovall. Mutual fund compliance officer independence and corporate governance. *Corporate Governance: An International Review*, 16(1):52–60, 2008.

[113] J. Holmstrom, M. Kitokivi, and A. P. Hameri. Bridging practice and theory: A design science approach. *Decision Sciences*, 40(1):65–87, 2009.

[114] D. Hong, M. Yuan, and V. Y Shen. Dynamic privacy management: a plug-in service for the middleware in pervasive computing. pages 1–8, 2005.

[115] K. Hui, H. H Teo, and S. Lee. The value of privacy assurance: an exploratory field experiment. *Management Information Systems Quarterly*, 31(1):19–33, 2007.

[116] Lotfi Hussami. A decision-support system for IS compliance management. In *Proceedings of the CAISE 2009 Doctoral Consortium*, Amsterdam, 2009.

[117] Thomas Husson. Profiling your best mobile customers. Technical report, Forrester Research, Inc., July 2010.

[118] P. G Inglesant and M. A Sasse. The true cost of unusable password policies: password use in the wild. In *Proceedings of the 28th international conference on Human factors in computing systems*, pages 383–392, New York, NY, USA, 2010.

[119] Innocentive. Challenge driven innovation. https://www.innocentive.com/seekers/challenge-based-innovation, 2010.

[120] Innocentive. For seekers. https://www.innocentive.com/how-it-works/seekers, 2010.

[121] Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK Guide).* Number 4th. PMI, Newtown Square, 2008.

[122] ISACA. Control objectives for information and related technology (COBIT) 4.1. Technical report, 2007.

[123] ISO. 9001 quality management systems - requirements. Technical report, 2008.

[124] ISO/IEC. 27001 information technology – security techniques – information security management systems - requirements. Technical report, 2005.

[125] ISO/IEC. 38500 corporate governance of information technology. Technical report, 2008.

[126] A.S.J.R. Joha. *The Retained Organization after IT outsourcing. The Design of its Organizational Structure*. PhD thesis, Faculty of Technology, Policy and Management. Delft University of Technology, 2003.

[127] I. Jureta, A. Siena, J. Mylopoulos, A. Perini, and A. Susi. Theory of regulatory compliance for requirements engineering. *Arxiv preprint arXiv:1002.3711*, 2010.

[128] Randolph Kahn and Barclay Blair. *Information Nation: Seven Keys to Information Management Compliance*. Wiley, 2 edition, February 2009.

[129] D. Kahneman, P. Slovic, and A. Tversky. Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157):1124–1131, 1974.

[130] Khalid Kark. Calculating the cost of a security breach. Technical report, Forrester Research, Inc., April 2007.

[131] Khalid Kark, Mark Othersen, and Chris McClean. Defining IT GRC. Technical report, Forrester Research, Inc., December 2007.

[132] Hope Koch and Ulrike Schultze. Stuck in the conflicted middle: A Role-Theoretic perspective on B2B E-Marketplaces. *Management Information Systems Quarterly*, 35(1):123–146, March 2011.

[133] J. Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.

[134] A. A Lado, N. G Boyd, and S. C Hanlon. Competition, cooperation, and the search for economic rents: a syncretic model. *The Academy of Management Review*, 22(1):110–141, 1997.

[135] J. J Laffont and D. Martimort. *The theory of incentives: the principal-agent model*. Princeton Univ Pr, 2002.

[136] K. R. Lakhani. Innocentive.com. Technical Report Harvard Business Case no. 9-608-170, 2009.

[137] K. R. Lakhani and J. A. Panetta. The principles of distributed innovation. *Innovations: Technology, Governance, Globalization*, 2(3):97–112, 2007.

[138] Caroline Lancelot Miltgen. Devoilement de donnees personnelles et contreparties attendues en e-commerce : une approche typologique et interculturelle. *Systemes d'information et management*, 15(4):1–49, 2010.

[139] R. N Langlois. Transaction-cost economics in real time. *Industrial and corporate change*, 1(1):99–127, 1992.

[140] L. Lapointe and S. Rivard. A triple take on information system implementation. *Organization Science*, 18(1):89–107, 2007.

[141] G. T. Lau, S. Kerrigan, K. H. Law, and G. Wiederhold. An e-government information architecture for regulation analysis and compliance assistance. pages 461–470. ACM New York, NY, USA, 2004.

[142] E. Lewis and G. Millar. The viable governance model - a theoretical model for the governance of IT. In *Proc. of the 42nd Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 2009.

[143] Mario Lezoche and F Taglino. Business process driven solutions for innovative entrprise information systems. Paris, 2008.

[144] T.R. Lindlof and B.C. Taylor. *Qualitative Communication Research Methods*. Sage Publications, Inc, Thousand Oaks, CA, 2002.

[145] Zhan Liu, Riccardo Bonazzi, Boris Fritscher, and Yves Pigneur. Privacy-friendly business models for Location-Based mobile services. *Journal of Theoretical and Applied Electronic Commerce Research*, 6(2), August 2011.

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

[147] M.M. Maher. Tips for managing relationship with regulators. *ABA Bank Compliance*, 26(3):24–28, 2005.

[148] N. K Malhotra, S. S Kim, and J. Agarwal. Internet users' information privacy Concerns(IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[149] A S Manasdeep, D. S Jolly, A. K Singh, M. A Srivastava, and M. S Singh. A proposed model for data privacy providing legal protection by E-Court. *International Journal of Engineering Science and Technology*, 2(4):649 –657, 2010.

[150] S. T. March and G. F. Smith. Design and natural science research on information technology. *Decision Support Systems*, 15(4):251–266, 1995.

[151] Wolfgang Marekfia and Volker Nissen. Strategisches GRC-Management – grundzüge eines konzeptionellen bezugsrahmens. *Forschungsberichte zur Unternehmensberatung*, 2009(2):1–11, 2009.

[152] Aaron K. Massey, Paul N. Otto, Lauren J. Hayward, and Annie I. Anton. Evaluating existing security and privacy requirements for legal compliance. *Requirements Engineering*, 15(1):119–137, November 2009.

[153] M. Mawdesley, G. Long, S. Al-jibouri, and D. Scott. The enhancement of simulation based learning exercises through formalised reflection, focus groups and group presentation. *Computers & Education*, 56(1):44–52, January 2011. ACM ID: 1872200.

[154] Chris McClean. The changing nature of governance, risk, and compliance. *Computer World UK*, February 2009.

[155] Chris McClean. The forrester wave: Enterprise governance, risk, and compliance platforms, q3 2009. Technical report, 2009.

[156] Chris McClean, K. McNabb, and A. Dill. The GRC technology puzzle: Getting all the pieces to fit. Technical report, Forrester Research, Inc., February 2009.

[157] Chris McClean and Michael Rasmussen. Topic overview: Governance, risk and compliance. Technical report, Forrester Research, Inc., November 2007.

[158] S.L. Mitchell. A framework to help organisations drive principled performance. *International Journal of Disclosure and Governance*, 4(4):279–296, 2007.

[159] C. Moorman, G. Zaltman, and R. Deshpande. Relationships between providers and users of market research: the dynamics of trust within and between organizations. *Journal of marketing research*, 29(3):314–328, 1992.

[160] G. Muller and O. Terzidis. IT-Compliance und IT-Governance. *Wirtschaftsinformatik*, 50(5):341–343, 2008.

[161] S. Muller and C. Supatgiat. A quantitative optimization model for dynamic risk-based compliance management. *IBM Journal of Research and Development*, 51(3):295–308, 2007.

[162] Barry Murphy. eDiscovery best practices. Technical report, Forrester Research, Inc., September 2007.

[163] Barry Nalebuff and Adam Brandenburger. Co-opetition: Competitive and cooperative business strategies for the digital economy. *Strategy & Leadership*, 25(6):28–35, November 1997.

[164] K. Namiri and N. Stojanovic. A semantic-based approach for compliance management of internal controls in business processes. In *Proceedings of CAISE 2007 Forum*, 2007.

[165] E. O Navarro and A. Van Der Hoek. On the role of learning theories in furthering software engineering education. In *Ellis, H. J.C. ,Demurjian, S.A. and Naveda J. F., eds. Software Engineering: Effective Teaching and Learning Approaches and Practices*, pages 38–59. IGI Global, 2009.

[166] Nokia Siemens Networks. Privacy survey 2009. Technical report, Nokia Siemens Networks, 2009.

[167] D. H Nguyen and E. D Mynatt. Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems. 2002.

[168] I. Nonaka and G. Von Krogh. Tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory. *Organization Science*, 20(3):635–652, 2009.

[169] OECG. GRC capability model. Technical report, 2009.

[170] OECG. GRC-IT blueprint. version 1.0. Technical report, 2010.

[171] OGC. ITIL v.3. Technical report, 2007.

[172] Stephen O'Grady. SOA meets compliance: Compliance oriented achitecture. Technical report, Red Monk, August 2004.

[173] Chitu Okoli and Kira Schabram. A guide to conducting a systematic literature review of information systems research. 2010.

[174] Basel Committee on Banking Supervision. Compliance and the compliance function in banks. Technical report, Basel Committee on Banking Supervision, 2005.

[175] A. Osterwalder and Y. Pigneur. *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers.* Wiley, New York, NY, USA, 2009.

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

[177] Mark Othersen. Best practices: Maintaining an IT control framework. Technical report, Forrester Research, Inc., April 2008.

[178] Mark Othersen and Chris McClean. Consolidation looms for the IT GRC market. Technical report, 2009.

[179] L. Palen and P. Dourish. Unpacking privacy for a networked world. pages 129–136, Florida,USA, 2003.

[180] The European Parliament and the Council of the European Union. Directive 2006/43/EC of the european parliament and of the council. http://eur-lex.europa.eu, 2006.

[181] V. Pathak and L. Iftode. Byzantine fault tolerant public key authentication in peer-to-peer systems. *Computer Networks*, 50(4):579–596, 2006.

[182] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77, 2007.

[183] Dietmar Pfahl, Oliver Laitenberger, Gunther Ruhe, Jorg Dorsch, and Tatyana Krivobokova. Evaluating the learning effectiveness of using simulations in software project management education: results from a twice replicated experiment. *Information and Software Technology*, 46(2):127–147, February 2004.

[184] J. Phelps, G. Nowak, and E. Ferrell. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1):27–41, 2000.

[185] Larry Ponemon. Privacy risk management. presentation for the national council of higher education loan programs, June 2000.

[186] Michael E. Porter. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. Free Press, 1 edition, June 1998.

[187] M. Pozzebon and A. Pinsonneault. Global-local negotiations for implementing configurable packages: The power of initial organizational decisions. *The Journal of Strategic Information Systems*, 14(2):121–145, 2005.

[188] PricewaterhouseCoopers. Integrity-Driven performance. a new strategy for success through integrated governance, risk and compliance management. Technical report, 2004.

[189] J. Pries-Heje, R. Baskerville, and J. Venable. Strategies for design science research evaluation. Galway, Ireland, 9-11 June 2008, June 2008.

[190] R. M. Purdy. Compliance initiatives can yield IT opportunities. *US Banker. Retrieved from http://www. americanbanker. com/article. html*, 2006.

[191] N. Racz, E. Weippl, and A. Seufert. A frame of reference for research of integrated governance, risk and compliance (GRC). In *Proceedings of Communications and Multimedia Security*, pages 106–117, 2010.

[192] Nicolas Racz, E Weippl, and Riccardo Bonazzi. IT governance, risk and compliance (GRC) status quo and integration. In *Proceedings of the First International Workshop on IT Governance, Risk and Compliance (ITGRC 2011)*, Washington D.C., July 2011.

[193] Nicolas Racz, E. Weippl, and A. Saufert. A process model for integrated IT governance, risk, and compliance management. In *Proc. of the Ninth International Baltic Conference (DB&IS 2010)*, Riga, 2010.

[194] Nicolas Racz, E. Weippl, and A. Saufert. Questioning the need for separate IT risk management frameworks. In *Proceedings of Informatik 2010*, Leipzig, Germany, 2010.

[195] Nicolas Racz, E. Weippl, and A. Saufert. Governance, risk and compliance (GRC) software – an exploratory study of software vendor and market research perspectives. In *Proc. 44th Hawaii International Conference on System Sciences (HICSS 2011)*, 2011.

[196] R. Radner. Costly and bounded rationality in individual and team decision-making. *Industrial and Corporate Change*, 9(4):623– 655, 2000.

[197] R. Radner and J. Marschak. Note on some proposed decision criteria. *Decision processes*, pages 61–68, 1954.

[198] B. Rao and L. Minakakis. Evolution of mobile location-based services. *Communications of the ACM*, 46(12):61–65, 2003.

[199] Michael Rasmussen. Seven habits of highly effective compliance programs. Technical report, Forrester Research, Inc., July 2005.

[200] Michael Rasmussen. Overcoming risk and compliance myopia. Technical report, Forrester Research, Inc., August 2006.

[201] Michael Rasmussen. 2008 GRC drivers, trends & market directions. Technical report, 2008.

[202] M. Rath and R. Sponholz. *IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen*. Schmidt, Berlin, 2009.

[203] J. Reagle and L. F Cranor. The platform for privacy preferences. *Communications of the ACM*, 42(2):55, 1999.

[204] J. K Rempel and J. G Holmes. How do i trust thee. *Psychology today*, 20(2):28–34, 1986.

[205] P. Ribbers, R. Peterson, and M. Parker. Designing information technology governance processes: diagnosing contemporary practices and competing theories. In *Proc. of the 35th Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 2002.

[206] Andre Rifaut. Goal-Driven requirements engineering for supporting the ISO 15504 assessment process. software process improvement. In *Proceedings of the 12th European Conference, EuroSPI 2005*, Budapest, Hungary, 2005.

[207] Andre Rifaut and C Faltus. Improving operational risk management system by formalizing the basel II regulation with goal models and the ISO/IEC 15504 approach. Technical report, 2006.

[208] M. Rosemann, I. Vessey, and R. Weber. Alignment in enterprise systems implementations: the role of ontological distance. In *In ICIS 2004 Proceedings. Twenty Fifth International Conference on Information Systems ICIS 2004, Washington, DC.*, pages 439–447, December 2004.

[209] M. B Rosson and J. M Carroll. *Usability engineering: scenario-based development of human-computer interaction*. Morgan Kaufmann Pub, 2002.

[210] Ron Sanchez and Aime Heene. *The New Strategic Management: Organization, Competition, and Competence*. Wiley, July 2003.

[211] C. Sauer and B. H Reich. Rethinking IT project management: Evidence of a new mindset and its implications. *International Journal of Project Management*, 27(2):182–193, 2009.

[212] L. J Savage. *The foundations of statistics*. Dover Pubns, 1954.

[213] B. Schilit, N. Adams, R. Want, et al. Context-aware computing applications. In *First workshop of Mobile Computing Systems and Applications*, pages 85–90, Santa Cruz, California, USA, 1994.

[214] F. Sebastiani. Machine learning in automated text categorization. *ACM computing surveys (CSUR)*, 34(1):1–47, 2002.

[215] Maung K Sein, Ola Henfridsson, Sandeep Purao, Matti Rossi, and Rikard Lindgren. Action design research. *MIS Quarterly*, 35(1):37–56, 2011.

[216] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer. Google android: A comprehensive security assessment. *IEEE Security & Privacy*, 8(2):35–44, March 2010.

[217] H. Sheng, F. F.H Nah, and K. Siau. An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, 9(6):344–376, 2008.

[218] B. H Sheppard, J. Hartwick, and P. R Warshaw. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, pages 325–343, 1988.

[219] A. Sheth. Enterprise applications of semantic web: The sweet spot of risk and compliance. *Industrial Applications of Semantic Web*, pages 47–62, 2005.

[220] A. Siena, J. Mylopoulos, A. Perini, and A. Susi. From laws to requirements. *Requirements Engineering and Law, 2008. RELAW'08.*, pages 6–10, 2008.

[221] Caroline Simard and Joel West. Knowledge networks and geopgraphic locus of innovation. In *Open Innovation: Researching a New Paradigm.* October 2005.

[222] Herbert A. Simon. A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1):99–118, February 1955. ArticleType: primary_article / Full publication date: Feb., 1955 / Copyright © 1955 The MIT Press.

[223] T. Sitzmann. A meta-analytic examination of the instructional effectiveness of computer-based simulation games. *Personnel Psychology*, 64(2):489–528, 2011.

[224] C. Skinner. Forensically evolving regulations. http://www.thefinanser.co.uk/2008/09/forensically-ev.html, 2008.

[225] K. Smith and C. Kampf. Developing writing assignments and feedback strategies for maximum effectiveness in large classroom environments. In *Professional Communication Conference, 2004. IPCC 2004. Proceedings. International*, pages 77–82, Minneapolis, Minnesota, USA, 2004.

[226] J. Y Son and S. S Kim. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32(3):503–529, 2008.

[227] M. Spence. Signaling in retrospect and the informational structure of markets. *American Economic Review*, 92(3):434–459, 2002.

[228] James Sterngold. Say goodbye to all those passwords. *BusinessWeek: Online Magazine*, January 2011.

[229] K. A Stewart and A. H Segars. An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1):36–49, 2002.

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

[231] R. I Sutton and B. M Staw. What theory is not. *Administrative Science Quarterly*, 40(3):371–384, 1995.

[232] E. B Swanson. Consultancies and capabilities in innovating with IT. *The Journal of Strategic Information Systems*, 19(1):17–27, 2010.

[233] Anthony Tarantino. *The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices.* Wiley, March 2008.

[234] A. Teubner and T. Feller. Informationstechnologie, governance und compliance. *Wirtschaftsinformatik*, 50(5):400–407, 2008.

[235] Her Majesty Treasury. The orange book. *Management of risk-principles and concepts. Norwich: HMSO*, 2004.

[236] Economist Intelligence Unit. Regulatory risk: Trends and strategies for the CRO. Technical report, Economist Intelligence Unit, 2005.

[237] V. K. Vaishnavi and W. Kuechler Jr. *Design science research methods and patterns: innovating information and communication technology.* Auerbach Pub, 2007.

[238] J. E. van Aken. Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules. *Journal of Management Studies*, 41(2):219–246, 2004.

[239] A. H. Van de Ven and M. S. Poole. Explaining development and change in organizations. *Academy of management review*, pages 510–540, 1995.

[240] A. Van Lamsweerde. Goal-oriented requirements engineering: A guided tour. pages 249–262, 2002.

[241] R. Van Rooy. Quality and quantity of information exchange. *Journal of Logic, Language and Information*, 12(4):423–451, 2003.

[242] W. Vanhaverbeke. The inter-organizational context of open innovation. In *Open Innovation: Researching a New Paradigm*, pages 205–219. 2006.

[243] V. Venkatesh. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research*, 11(4):342–365, 2000.

[244] Viswanath Venkatesh, Michael Morris, Gordon Davis, and Fred Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3):425–478, September 2003.

[245] L. Volonino, G. H. Gessner, and G. F. Kermis. Holistic compliance with Sarbanes-Oxley. *The Communications of the Association for Information Systems*, 14(1):457–468, 2004.

[246] Steve Wagner and Mark Layton. The two faces of risk. http://www.deloitte.com/, August 2007.

[247] Ron Weber. Theory building in the information systems discipline: Some critical reflections. Canberra, Australia, September 2010.

[248] A. Wegmann. On the systemic enterprise architecture methodology (SEAM). In *Proceedings of the International Conference on Enterprise Information Systems (ICEIS) 2003*, 2003.

[249] A. Wegmann, G. Regev, and B. Loison. Business and IT alignment with SEAM. 2005.

[250] P. Weill and J. Ross. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press, Boston, MA, 2004.

[251] G. M Weinberg and D. Weinberg. *General principles of systems design*. Dorset House, 1988.

[252] Andreas Werr and Torbjorn Stjernberg. Exploring management consulting firms as knowledge systems. *Organization Studies*, 24(6):881 –908, July 2003.

[253] J. West and S. Gallagher. Challenges of open innovation: the paradox of firm investment in open-source software. *R&D Management*, 36(3):319–331, 2006.

[254] R. Whittington. Strategy practice and strategy process: family differences and the sociological eye. *Organization Studies*, 28(10):1575–1586, 2007.

[255] M. Wiesche, M. Schermann, and H. Krcmar. Exploring the contribution of information technology to governance, risk, and compliance (Grc) initiatives,. In *Proceedings of the 19th European Conference on Information Systems (ECIS)*, Helsinki, Finland., June 2011.

[256] O. E Williamson. Comparative economic organization: The analysis of discrete structural alternatives. *Administrative science quarterly*, 36(2), 1991.

[257] Oliver Williamson. Strategy research: Governance and competence perspectives. *Strategic Management Journal*, 20(12):1087–1108, 1999.

[258] Oliver E. Williamson. The theory of the firm as governance structure: From choice to contract. *The Journal of Economic Perspectives*, 16(3):171–195, July 2002. ArticleType: research-article / Full publication date: Summer, 2002 / Copyright © 2002 American Economic Association.

[259] H. Yu, P. B Gibbons, M. Kaminsky, and F. Xiao. Sybillimit: A near-optimal social network defense against sybil attacks. In *2008 IEEE Symposium on Security and Privacy*, page 3–17, 2008.

[260] C. M Zapata. A classroom game for teaching management of software companies. *Dyna*, 77(163):290–299, 2010.

[261] M. Zur Muehlen and Michael Rosemann. Integrating risks in business process models. In *Proceedings of Aus- tralasian Conference on Information Systems*, Sydney, Australia, 2005.