Managing legal compliance through security requirements across service provider chains: A case study on the German Federal Data Protection Act

Christian Sillaber, Ruth Breu*
Quality Engineering Research Group
Institute of Computer Science, University of Innsbruck
Technikerstrasse 21a, A-6020 Innsbruck
{christian.sillaber, ruth.breu}@uibk.ac.at

Abstract: Future service customer-provider as well as inter-provider relationships will see the increased application of dynamic service composition providing a broad diversity of functions. However, currently existing deficiencies of processes and tools force service providers and service consumers to trade off profitability against security compliance. This is predominately due to the ignorance or manual resolution of policy and configuration dependencies, caused by distinct terminologies and languages used at both the service provider and service customer. We report on the research design for the Collaborative Security Requirement Management System (CoSeRMaS), a collaborative and semi-automated tool to manage, define and validate inter organizational requirements. We demonstrate the capabilities of CoSeRMaS to establish and validate the legal compliance that is demanded by the German Bundes Datenschutzgesetz (BDSG) when two or more customers and providers exchange data as part of their service composition.

1 Introduction

Service providers strive to improve the quality of the service they provide. To achieve a high level of quality, it is often required to rely on third parties for data processing. Therefore, sensitive data that has been provided by the service customer is often shared with third parties. Accidental disclosure of this information may often negatively affect the customer's life or business. To prevent this, governments have established legislations to ensure that privacy is respected and businesses processing data must comply with it. For example, the German Bundesdatenschutzgesetz (BDSG), protects personal information from being disclosed to unauthorized third parties and defines specific compliance rules for business entities processing such data.

Future customer-service provider relationships will see the increased application of dynamic service composition providing a broad diversity of functions. Service providers

*This work was partially funded by the European Commission under the FP7 project "PoSecCo" (IST 257129).

themselves will become service customers, as they will increasingly become part of more complex service orchestrations. As a result, service providers are faced with three challenges: First, to ensure internal compliance to relevant privacy laws. Second to ensure the compliance of third parties they rely on for data processing. And third, to communicate the state of compliance in a timely, correct and understandable manner to either the customer directly or other providers across the service composition chain.

Recent research on bridging the gap between formal concepts and legal texts has either focused on first-order temporal logic (e.g. [BMDS07, BKM10, DJL08, LM09]) or descriptive languages (e.g. [JSS01, LMW02, MGL06]). Despite this huge number of frameworks and formal concepts, to the best of our knowledge, there has been comparatively little work on actually using formalized legal texts to improve business processes, inter-business and customer-business relationships. The lack of profound tool support for ensuring legal compliance of day-to-day business processes through formalized legal texts is a significant deficiency, if the idea is to succeed in tomorrow's service organizations. The contributions of our work are intended to help bridge this gap.

The main contribution of this paper is threefold: First, we have formalized the BDSG using a requirement fulfillment model. Secondly, we have developed the Collaborative Security Requirement Management System (CoSeRMaS) prototype, as a collaborative and semi-automated tool to define, validate and exchange intra organizational security requirements. CoSeRMaS helps service providers to ensure that their business complies with applicable laws and policies. It furthermore enables businesses that are part of service composition chains to efficiently and transparently communicate their internal compliance with the law and ensure and manage the compliance state of third parties they rely on. Finally, we use the formalization of the BDSG to show how CoSeRMaS can be used to assure BDSG compliance along a chain of service providers in a small case study.

2 Related work

In [HOA06], the authors present the requirement based access control analysis and policy specification method. The presented method integrates access control analysis to ensure a policy and requirements compliant system. A set of process descriptions and heuristics are presented that support analysts derive and specify access control policies while ensuring traceability. However, the presented approach focuses on software development processes and not on general business processes or compliance along service provider chains. The approach we present in this paper provides a traceable approach to compliance mechanisms between business entities as well as internal processes.

Goal-based modeling is used by the authors of [Rif06] to verify the implementation of a financial system to ensure compliance with the Basel II regulation. The presented method divides the organization and its business processes in distinct organizational layers. Then, for each organizational layer, objectives, strategies and indicators are defined to provide a structure for the design of a regulation-compliant financial system. Apart from being design-oriented, the presented approach does not provide mechanisms to identify non-

compliance situations. Furthermore, their approach cannot be easily generalized and focuses on internal compliance.

Several methods have bee proposed in the past to formalize privacy laws. Most approaches (e.g. [BMDS07, BKM10, DJL08, LM09]) emphasize first-order logic models to derive legislative objectives. While these approaches work well for automated systems and processes, they lack support for higher level business processes. I.e. they can be used to validate a specific software tool for its compliance but do not provide adequate means beyond that on an organizational level. Furthermore, they do not provide traceability mechanisms and are often not designed for use by stakeholders.

Several Governance, Risk and Compliance (GRC) tools are currently available on the market that provide support for business wide compliance and risk management [Tar08]. While tools like Axentis [BH05], BWise [Spi11] or OpenPages [RWB11] provide support for risk and compliance management, their inner processes are often not publicized and their scientific validity is not verifiable [RWS11]. It is often unclear how well these tools support the functional model of the company or to what degree they require the company to align their business processes with a specific methodology [SG09, RWS11].

3 Motivation and definitions

Compliance with applicable laws is an important concern for organizations that collect and process personal information, such as service providers. The design and control of organizational processes that are compliant with privacy regulations has become one of the greatest challenges for service providers today (for example, health service providers [Dey10]).

It is apparent that the legal language and terminology used in laws like the BDSG is much too specific, dense and often too complicated to be used as a day-to-day guide to managers and decision makers of service providers [Dey10, PH10]. Instead, stakeholders as well as service customers are interested in straight answers to questions, such as "Is the service provider compliant to the BDSG?", "What has the service provider done/to-do to be compliant?" and "Can the service provider back up these claims with reliable data?". A recent study [TBDM12] has identified the proper coordination of the involved parties as well as the management of (security) relationships across orchestrated services as two key challenges in today's cross-organizational security management.

Therefore, to demonstrate the capabilities of CoSeRMaS and to address these challenges, as defined in [TBDM12], we want to answer the following question: *Is it possible to have efficient means of verifying whether a particular service provider (that is part of a complex service orchestration) is compliant to a specific law or regulation?* We have chosen the BDSG as the law of interest in this paper for three reasons: First, it is rather short with less than 50 paragraphs and second, this law does not require any particular domain knowledge unlike other (privacy) laws (e.g. HIPAA [Lad97]). Third, the law is not service provider specific, i.e. it applies as a lex specialis to health care service providers as well as generic data processing service providers.

For the scope of this paper we understand *compliance with the BDSG* as fulfilling all legal

requirements defined in the BDSG. For simplicity we view the BDSG as an isolated law and do not consider any other norms that might apply. *Legal requirements* are used in this paper to describe all conditions or capabilities that must be met or possessed by the business entity to satisfy the BDSG, i.e. be compliant with the BDSG (cf. [Kot92]). A legal requirement is *fulfilled*, if all conditions or capabilities are, in fact, met or possessed by the business entity. For instance, the legal requirement of § 4e BDSG (content of report to legal authority) is fulfilled, if the report sent to the legal authority contains the nine entries defined in § 4e BDSG.

4 CoSeRMaS and the BDSG: a case study

Consider a simple motivating scenario in which a customer wants to process complex and sensitive data. Rather than purchasing his/her own infrastructure to run the calculation, he/she decides to rely on a service provider to do the processing. However, as it turns out, the service provider is not capable of doing the entire processing in house and has to rely on a third party service provider. The service customer is aware of this situation, but requires the service provider to ensure that the third party is fully BDSG compliant. Figure 1 shows the three parties. Service Provider 1 relies on three Services (1, 2, 3). Service 1 processes the sensitive data. The other services do not process sensitive data. The dotted arrows denote how sensitive data is provided from the customer to the first service provider and from there to the second service provider (flow of processed data not shown). The flow of compliance information is show as a bold arrow: The third party (Service Provider 2) has to report its internal compliance state to Service Provider 1, which then has to store and report it in combination with the state of its internal BDSG compliance to the service customer.

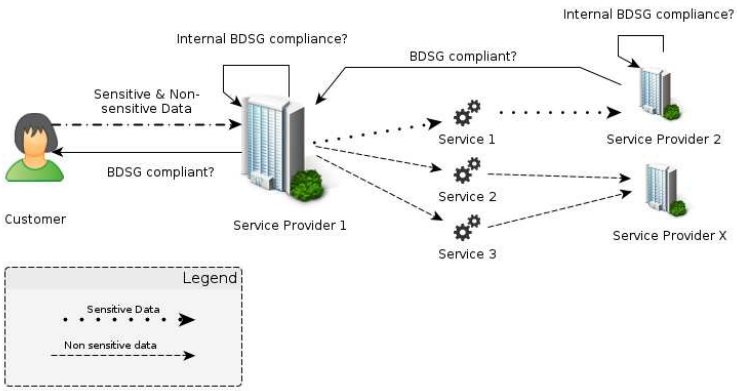

Figure 1: Motivating scenario: Ensuring BDSG compliance across a service provider chain

4.1 CoSeRMaS

CoSeRMaS [BFIO+11] has been developed to improve the management of security requirements. It has been designed to manage internal security requirements derived from laws, policies or other requirements. The tool provides stakeholders with a convenient interface to view, specify and refine requirements. The confirmation status of requirements can either be set manually by stakeholders, or CoSeRMaS can automatically set them according to the results of external scripts (e.g. results of a database query). Furthermore, it allows to verify and manage the delegation of responsibilities among employees. E-mail capabilities and an internal task and messaging system allow for the easy exchange of information between stakeholders. CoSeRMaS can send automatic requests for the requirement confirmation via e-mail to stakeholders outside organizational bounds.

Built around the generalized concept of security requirements [HB09,IOB06], CoSeRMaS can be used to freely model requirement fulfillment trees. The underlying meta-model is depicted in Figure 2. The central components of the meta-model are the Security Requirements and the Protection Targets. Security Requirements are derived from a Source, for instance the BDSG. Each Security Requirement is linked to a Protection Target, i.e. an asset it protects.

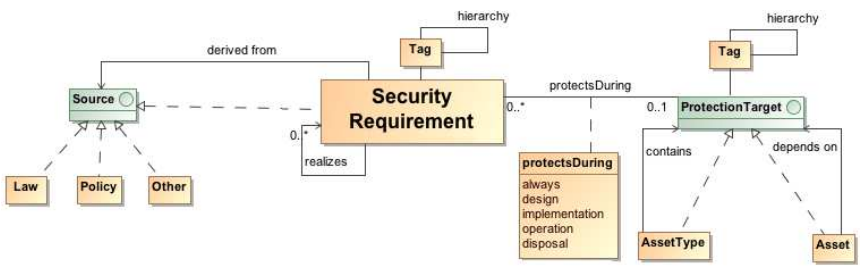

Figure 2: Simplified meta-model used by CoSeRMaS.

AssetTypes can be used to group assets together. For instance, in our example the AssetType, *External IT Services* contains three assets: *Service 1*, *Service 2* and *Service 3* (cf. Figure 3). Through the attribute *BDSG-Sensitive-Data* = {*true / false*}, external services that process sensitive data, and therefore have to be BDSG compliant, can be marked. The overall structure of the protection targets can be derived from the functional model of the organization (cf. [BFIO+11] for detailed information on the meta-model and the connection to the functional model).

For the scope of this paper, we define requirement *fulfillment trees* analogous to directed, acyclic graphs: A fulfillment tree is an ordered pair $F = (R, A)$ with R being a set of requirements and A being a set of requirement fulfillment connections. A requirement fulfillment connection $a = (x_1, x_2, \ldots, x_n, y, FM)$ denotes that the fulfillment of requirement y depends on the fulfillment of requirements $x_1, x_2, \ldots, x_n$ and the associated fulfillment model FM. The fulfillment model describes a function that determines the fulfillment status of a superordinate requirement based on the fulfillment status of subordinate requirements. For example, let the fulfilment model be the logical AND (i.e. all

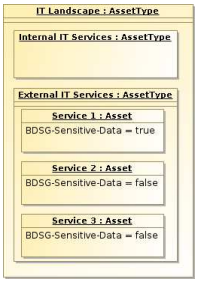

Figure 3: Protection Targets from our case study that model an IT Service Landscape with three external IT services.

subordinate requirements have to be fulfilled in order to fulfill the superordinate requirement):

$$FM(y) = \begin{cases} \text{not fulfilled} & \text{otherwise} \end{cases}$$

The function $state(x_i)$ returns the fulfillment status of the requirement x_i. If x_i is a superordinate requirement, the status depends on the evaluation of the subordinate requirements according to the above description. If x_i is a subordinate requirement, the status has to be either set manually by a stakeholder or is set automatically according to the value returned by an external script that was executed by CoSeRMaS. Although the resulting fulfillment tree is - mathematically speaking - a graph, we decided to refer to it as tree due to the clear structure and precedence between requirements that results form the fulfillment model. If, in the following sections no specific FM is mentioned, an AND connection of subordinate requirements is implied.

4.2 Deriving requirements from the BDSG

As outlined in 4.1, CoSeRMaS has been developed to manage security requirements. The challenge is now to transfer the BDSG according to a methodical approach to security requirements.

The first, and trivial step is to introduce *BDSG compliance* as a security requirement. According to the concept of fulfillment models, outlined in the previous section we can then proceed to model the BDSG - requirement and fulfillment tree in CoSeRMaS by breaking down the overall requirement in smaller, better manageable requirements.

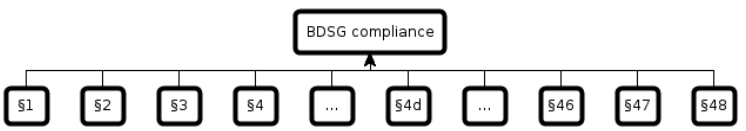

Figure 4: Flat security requirements derived from the BDSG.

The BDSG consists of 48 paragraphs that can be used to further refine the overall compliance requirement. Following the notation defined in the previous section, this flat fulfillment tree can be defined as $BDSG_{\text{compliant}} = (1, 2, 3, \ldots, 47, 48, AND)$ (cf. Figure 4). However, this simple fulfillment and requirement tree is far from being useful. For instance, not all paragraphs contain normative rules. E.g. § 1 BDSG contains legal definitions and terminology. Similarly, §§ 45ff BDSG contain transitional provisions. Therefore, to generate a useful fulfillment tree, we conducted a throughout analysis the BDSG. During this analysis, we have identified three types of fulfillment models. They are shortly described with an illustrating example in the following paragraphs.

In the first fulfillment model, a paragraph requires one, two or more paragraphs to hold true (AND case) . For instance, § 6 BDSG requires the business to ensure the rights of affected persons according to §§ 19, 34 BDSG (right of information) and §§ 20, 35 BDSG (right of correction, removal or locking of data). Therefore, § 6 BDSG is only fulfilled if measures according to §§ 19, 34, 20, 35 BDSG are in place (cf. Figure 5)

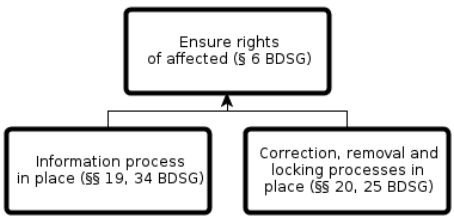

Figure 5: Example for an AND - Fulfillment model in the BDSG: The top level security requirement is fulfilled if all low level requirements are fulfilled.

Second fulfillment case: a paragraph contains two or more alternative cases. For instance, §4 d 3) BDSG exempts companies with less than 9 employees from the reporting obligation according to §4 d BDSG. Therefore, to be compliant with §4 d BDSG, a company has to either report to the authorities according to §4 d 1) BDSG, or have a commissioner for data protection appointed according to § 4d 2) BDSG or must fulfill the conditions of § 4d 3) BDSG (cf. Figure 6).

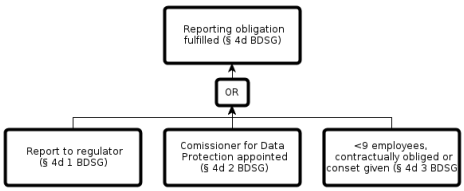

Figure 6: Example for an OR - Fulfillment model in the BDSG: The top level security requirement is fulfilled if at least one subordinate requirement is fulfilled.

The third type of fulfillment is the *basic* type which denotes a leaf requirement. This requirement is either set to fulfilled or not fulfilled by a human or a computer script that

verifies the requirement against reality. For instance, § 4e BDSG determines the content of a report to the regulatory authority. It consists of 9 entries that must be included in each report (e.g. name of company, address, etc.). Each of these entries is a leaf node of the *Report well formed (§ 4e BDSG)* requirement that connects them via an AND fulfillment rule.

Based on these findings, we transformed the BDSG in a fulfillment tree, depicted in Figure 7. Due to limited space we have only included the first three levels that include the important cases AND, OR and leaf requirement.

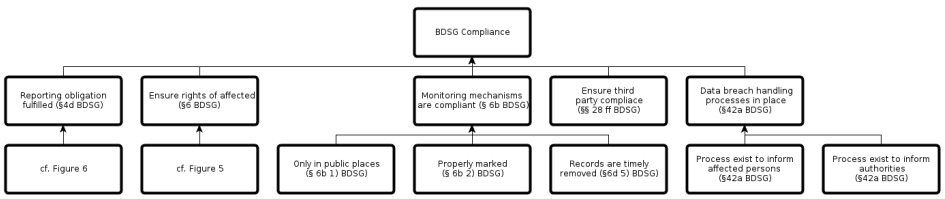

Figure 7: First three levels of the BDSG compliance requirement tree.

Our formalization of the BDSG showed, that out of the 66 paragraphs contained in the law, 25 specify requirements relevant to the scope of this paper.

- Paragraphs that do not contain requirements (but terminology or transition rules) (13): §§ 1, 2, 3, 38-38a, 39, 40, 41, 42, 45-48 BDSG.
- Paragraphs that either contain targeted provisions or penalties (8): §§ 3a, 4, 4a, 4b, 4c, 7, 43, 44 BDSG.
- Paragraphs that address public bodies, not private entities (6): §§ 8, 12, 23-26 BDSG.
- Paragraphs that contain relevant security requirements (25): §§ 4d, 4e, 4f, 4g, 5, 6, 6a, 6b, 6c, 9a, 10, 11, 27-35, 42a BDSG.

4.3 Managing BDSG compliance from within CoSeRMaS

In our small case study, Service Provider 1 (cf. Figure 1) uses the CoSeRMaS tool to manage its security requirements. The tool provides the service provider with a template of the BDSG according to our formalization, presented in Section 4.2.

After importing the BDSG requirement tree, it is shown in the CoSeRMaS application and the responsible person can further refine the requirement tree (cf. Figure 9). This requires either the assignment of requirements to specific stakeholders responsible for the validation and fulfillment of the requirement (e.g. privacy protection officer), linking the particular requirement to a script or an external data source (e.g. importing the fulfillment tree from Service Provider 2), or creating additional subordinate requirements.

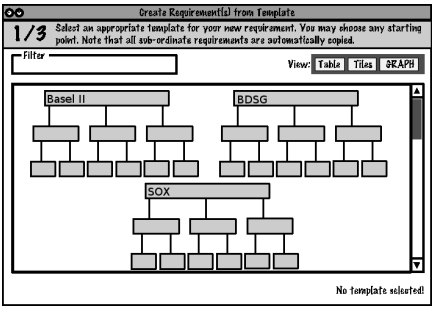

Figure 8: CoSeRMaS template dialog that allows users to import the BDSG requirement tree.

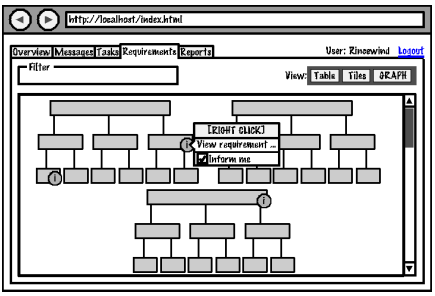

Figure 9: CoSeRMaS dashboard, showing the formalized BDSG requirements tree.

In our case, some requirements have to be revalidated after a certain time has passed. For instance, the third party compliance has to be verified in sensible intervals. Also, the timely removal of video surveillance tapes has to be ensured frequently. To support this recurring task of re-validating requirements, CoSeRMaS provides a scheduler service. This scheduler service re-runs scripts for the automatic validation of requirements and informs users if requirements, they are responsible for, are about to expire.

After importing the BDSG security requirements, employees responsible for realizing the requirements are assigned to their specific requirements and their respective status can be tracked from within the tool.

In our scenario, the stakeholder for managing third party compliance refines the *Ensure third party compliance (§§ 28 ff BDSG)* requirement to include a subordinate requirement, *Service Provider 2 is BDSG compliant*. The fulfillment of this newly created requirement is then linked to the top-level requirement *BDSG compliance* of Service Provider 2. Currently, this is done via mail where a designated recipient at service provider two receives a questionnaire where he answers compliance questions with fulfilled/not fulfilled according to Figure 7. In a future version, the CoSeRMaS instance of service provider 1 will be able to directly communicate with the CoSeRMaS instance of Service Provider 2 to automatically exchange the fulfillment status without any human interaction.

4.4 CoSeRMaS along the service chain

Now that Service Provider 1 has successfully managed and verified its compliance and integrated the data provided by Service Provider 2, he can now proceed to provide the customer with the required and demanded information.

This important step is supported by CoSeRMaS through two mechanisms. Either the customer is granted access to CoSeRMaS directly with a read-only account, or he is provided with a printed report. Currently two types of reports are provided by the tool: A tabular report that lists the fulfillment status of all security requirements grouped according to the hierarchy. And a time-based view can be generated that lists the fulfillment status of all requirements within given intervals (cf. Figure 10).

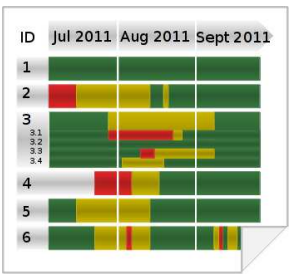

Figure 10: Timeline report: Shows the fulfillment model of each requirement within a specific interval. Can be used, depending on the granularity level either for the internal compliance evaluation or as a visual compliance report for customers.

CoSeRMaS provides several tangible benefits for service providers as well as customers along the service chain. First, reusing fulfillment trees improves the efficiency and consistency of compliance management along the value chain. Only when no formalized model of a law exists, or if a security requirement is too broadly defined, a security requirements engineer has to refine the existing fulfillment tree as well as the protection target model. Second, CoSeRMaS automatically establishes the traceability link between security requirements and the laws they are derived from. This helps customers, internal and external stakeholders to easily verify the source and purpose of each requirement. If a requirement is manually refined by a stakeholder, refined elements automatically inherit the source of the parent requirements. Through this automatic inheritance and visual support provided by the fulfillment tree, requirements can easily verified by stakeholders without a legal background. Third, the fulfillment tree based approach enables a quick identification of the overall compliance status as well as the fast identification of non fulfilled requirements. Finally, upon completion of the tool, additional views, reports and support for an OCL-like query language will enable the fast customization of CoSeRMaS to fit various needs and different use cases. Service Provider will be able to create audit specific views to allow for the thorough audit of their internal processes by an auditor. Through the direct link between requirements and protection targets, it is possible to create views that present an auditor with data on specific IT services, depending on their attribute(s).

5 Conclusion and future work

We have presented a requirement based formalization approach for legal texts and used it to formalize the BDSG. Furthermore, we have shown how this formalization can be used by a collaborative security requirements management system to ensure, communicate and manage compliance with legislation in general, and the BDSG in particular. On the example of a service provider chain we demonstrated how our tool can be used to manage and communicate the state of legal compliance across several businesses that are part of a service chain. By using CoSeRMaS for the management of security requirements, businesses can ensure the timely and correct management of requirements in compliance with specific laws.

Nonetheless, security requirement based assurance of legal compliance would benefit from future work in two directions. First, increasing the number of formalized legal texts would reduce the work required from businesses drastically. For this, further support (e.g. support for semantic annotations, legal data mining) tools and formalization techniques (e.g. ontologies for laws) have to be developed to assure a correct formalization of large legal texts. Second, standardized means of communicating compliance information would aid businesses. Also, customers could benefit from a standard by improving the decision making process when deciding which service provider to include in a service orchestration.

References

[BFIO+11] Ruth Breu, Matthias Farwick, Frank Innerhofer-Oberperfler, Michael Brunner, Klaus Julisch, and Günter Karjoth. D2.1 A Framework for Business Level Policies. Technical Report 257129, PoSecCo project (project no 257129), 7th Framework Programme for R&D (FP7), 2011.

[BH05] N.A. Bagranoff and L. Henry. Choosing and Using Sarbanes-Oxley Software. *Information Systems Control Journal 2*, pages 49–51, 2005.

[BKM10] David Basin, Felix Klaedtke, and Samuel Müller. Monitoring Security Policies with Metric First-order Temporal Logic. *Control 12*, pages 23–33, 2010.

[BMDS07] Adam Barth, John Mitchell, Anupam Datta, and Sharada Sundaram. Privacy and Utility in Business Processes. *20th IEEE Computer Security Foundations Symposium CSF07 5*, pages 279–294, 2007.

[Dey10] Henry Deyoung. Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws. *Public Policy 9*, pages 73–82, 2010.

[DJL08] Nikhil Dinesh, Aravind Joshi, and Insup Lee. Reasoning about conditions and exceptions to laws in regulatory conformance checking. *Deontic Logic in Computer, 9*, pages 110–124, 2008.

[HB09] M. Hafner and R. Breu. *Security engineering for service-oriented architectures*. Springer-Verlag New York Inc, 2009.

[HOA06] Qingfeng He, Paul Otto, and AI Anton. Ensuring compliance between policies, requirements and software design: A case study. *Information Assurance 9*, pages 209–221, 2006.

[IOB06] F. Innerhofer-Oberperfler and R. Breu. Using an enterprise architecture for IT risk management. In *Information Security South Africa Conference, ISSA*, 2006.

[JSS01] S Jajodia, P Samarati, and ML Sapino. Flexible support for multiple access control policies. *ACM Transactions 26:2*, pages 214–260, 2001.

[Kot92] Gerald Kotonya. Viewpoints for requirements definition. *Software Engineering Journal 9*, pages 71–81, 1992.

[Lad97] Kala Ladenheim. Health Insurance in Transition: The Health Insurance Portability and Accountability Act of 1996. *Publius 27*, pages 33–51, 1997.

[LM09] P Lam and J Mitchell. A formalization of HIPAA for a medical messaging system. *Trust, Privacy and Security in Digital Environments 11*, pages 73–85, 2009.

[LMW02] Ninghui Li, John C Mitchell, and William H Winsborough. Design of a Role-based Trust-management Framework. *Symposium A Quarterly Journal In Modern Foreign Literatures*, pages 104–113, 2002.

[MGL06] Michael J May, Carl A Gunter, and Insup Lee. Privacy APIs: Access Control Techniques to Analyze and Verify Legal Privacy Policies. *19th IEEE Computer Security Foundations Workshop CSFW06*, pages 85–97, 2006.

[PH10] A. Pfitzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *URL: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0 (Accessed 12.04.2012)*, pages 12–21, 2010.

[Rif06] André Rifaut. Improving operational risk management systems by formalizing the Basel II regulation with goal models and the ISO/IEC 15504 approach. *Proceeding, REMO2V*, pages 831–837, 2006.

[RWB11] N. Racz, E. Weippl, and R. Bonazzi. IT Governance, Risk & Compliance (GRC) Status Quo and Integration: An Explorative Industry Case Study. In *Services (SERVICES), 2011 IEEE World Congress on*, pages 429–436. IEEE, 2011.

[RWS11] N. Racz, E. Weippl, and A. Seufert. Governance, Risk & Compliance (GRC) Software-An Exploratory Study of Software Vendor and Market Research Perspectives. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1–10. IEEE, 2011.

[SG09] S. Sadiq and G. Governatori. *Handbook of Business Process Management*, chapter A methodological framework for aligning business processes and regulatory compliance. Springer, 2009.

[Spi11] M. Spies. A software assurance evidence approach to cloud security. In *Database and Expert Systems Applications (DEXA), 2011 22nd International Workshop on*, pages 39–43. IEEE, 2011.

[Tar08] A. Tarantino. *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*. Wiley, 2008.

[TBDM12] Stefan Thalmann, Daniel Bachlechner, Lukas Demetz, and Ronald Maier. Challenges in Cross-Organizational Security Management. *Hawaii International Conference on System Sciences*, pages 5480–5489, 2012.