Managing Regulatory Compliance in Business Processes

Shazia Sadiq and Guido Governatori

S. Sadiq
School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, QLD, Australia
e-mail: shazia@itee.uq.edu.au

G. Governatori
Software Systems Research Group, NICTA, Australia
email: guido.governatori@nicta.com.au

Abstract

The ever-increasing obligations of regulatory compliance are presenting a new breed of challenges for organizations across several industry sectors. Aligning control objectives that stem from regulations and legislation with business objectives devised for improved business performance is a foremost challenge. The organizational as well as IT structures for the two classes of objectives are often distinct and potentially in conflict. In this chapter, we present an overarching methodology for aligning business and control objectives. The various phases of the methodology are then used as a basis for discussing state-of-the-art in compliance management. Contributions from research and academia as well as industry solutions are discussed. The chapter concludes with a discussion on the role of BPM as a driver for regulatory compliance and a presentation of open questions and challenges.

1 Introduction

Compliance is defined as ensuring that business processes, operations, and practice are in accordance with a prescribed and/or agreed set of norms. Compliance requirements may stem from legislature and regulatory bodies (e.g., Sarbanes-Oxley, Basel II, HIPAA), standards and codes of practice (e.g., SCOR, ISO9000), and also business partner contracts. The market value for compliance-related software and services was estimated as over $32 billion in 2008 (Hagerty et al., 2008). The boost in business investment is primarily a consequence of regulatory mandates that emerged as a result of events, which led to some of the largest scandals in corporate history such as Enron, WorldCom (USA), HIH (Australia), and Societé Generale (France). In spite of

mandated deadlines, there is evidence that many organizations are still struggling with their compliance initiatives.

Compliance is historically viewed as a burden, although there are indications that businesses have started to see the regulations as an opportunity to improve their business processes and operations. Industry reports (BPM Forum, 2006) indicate that up to 80% of companies expect to reap business benefits from improving their compliance regimens.

In general, a compliance regimen must include three interrelated but distinct perspectives on compliance, namely, corrective, detective, and preventative.

Corrective measures can be undertaken for a number of reasons, ranging from the introduction of a new regulation impacting upon the business, to breech reporting, to the organization coming under surveillance and scrutiny by a control authority, or, in the worst case, to an enforceable undertaking. Corrective measures undertaken in a proactive manner, position the organization favorably with regulators or other control authorities.

Detective measures are undertaken under two main approaches. First is *retrospective reporting*, wherein traditional audits are conducted for "after-the-fact" detection, through manual checks by consultants and/or through IT forensics and business intelligence (BI) tools. A second and more recent approach is to provide some level of automation through *automated detection*. The bulk of existing software solutions for compliance follow this approach. The proposed solutions hook into a variety of enterprise system components (e.g., SAP HR, LDAP Directory, Groupware, etc.) and generate audit reports against hard-coded checks performed on the requisite system. These solutions often specialize in certain class of checks, for example, the widely supported checks that relate to Segregation of Duty violations in role management systems. However, this approach still resides in the space of "after-the-fact" detection, although the assessment time is reduced and correspondingly the time to remediation and/or mitigation of control deficiencies is also improved.

A major issue with the above approaches (in varying degrees of impact) is the lack of sustainability. Even with automated detection facility, the hard-coded check repositories can quickly grow to a very large scale, making it extremely difficult to evolve and maintain them for changing legislatures and compliance requirements. In addition to external pressures, there is often a company internal push toward quality-of-service initiatives for process improvement, which have similar requirements.

In this chapter, we promote the use of sustainable approaches for compliance management, which we believe should fundamentally have a preventative focus, thus achieving *compliance by design* (Sadiq et al., 2007). That is, compliance should be embedded into the business practice, rather than be seen as a distinct activity. In particular, we argue that a compliance-by-design approach that capitalizes on Business Process Management (BPM) techniques has the potential to include also detective and corrective measures, leading to a holistic and effective compliance regimen.

The fundamental feature of the compliance-by-design approach is the ability to capture compliance requirements through a generic requirements modeling framework, and subsequently facilitate the propagation of these requirements into business process models and enterprise applications.

The biggest challenges in this regard is aligning control objectives that stem from regulations and legislation, with business objectives devised for improved business performance (KPMG

Advisory, 2005). The organizational as well as IT structures for the two classes of objectives are often distinct and potentially in conflict.

This chapter is dedicated to developing an understanding of the issues and challenges found in achieving the alignment between business and control objectives.

To this end, we will first introduce a guiding scenario in order to establish basic terms and concepts. We then present an overarching methodology for compliance management that focuses on aligning business and control objectives. The methodology demonstrates the use of Business Process Management and related technologies as a driver for managing compliance and is primarily intended to achieve compliance by design. Using the methodology as a basis for discussion, we will then provide a discussion on recent developments in compliance management services and solutions covering contributions from both academia as well as industry. We further present a brief case study targeted at 2 specific phases of the methodology. The analysis of current solutions as well as the case study indicate that a process-driven approach to compliance management is a highly effective way to address this complex problem. The chapter concludes with a discussion on open questions and challenges toward effective compliance management.

2 Scenario and Background

Consider the following example. In 2006, a new legislative framework was put in place in Australia for anti-money laundering. The first phase of reforms for the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF) covers the financial sector including banks, credit unions, building societies, and trustees, and extends to casinos, wagering service providers, and bullion dealers. The AML/CTF act imposes a number of compliance obligations or *control objectives*, which include the following:

- Customer due diligence (identification, verification of identity, and ongoing monitoring of transactions)
- Reporting (suspicious matters, threshold transactions, and international funds transfer instructions)
- Record keeping
- Establishing and maintaining the AML/CTF program

AML/CTF is a *principles-based*[1] regulation, and hence, businesses need to determine the exact manner in which they will fulfill the obligations. This leads to the design of so-called internal controls[2] devised by a particular financial organization. For example, consider an account-opening process as depicted in Fig 1. An internal control may mandate the "scanning of all new customer accounts against blocked entity datasets" in response to the obligation to provide

[1] "The AML/CTF Act is a principles-based piece of legislation. It sets out broad obligations which reporting entities and others affected by the legislation must meet, but leaves the methods of meeting those obligations to be decided by those on whom the obligations fall" (AUSTRAC, 2006).

[2] "Internal control is broadly defined as a process effected by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations" (COSO, 1994).

customer due diligence during the account-opening process. This would require an additional check to be conducted after entering new customer information.

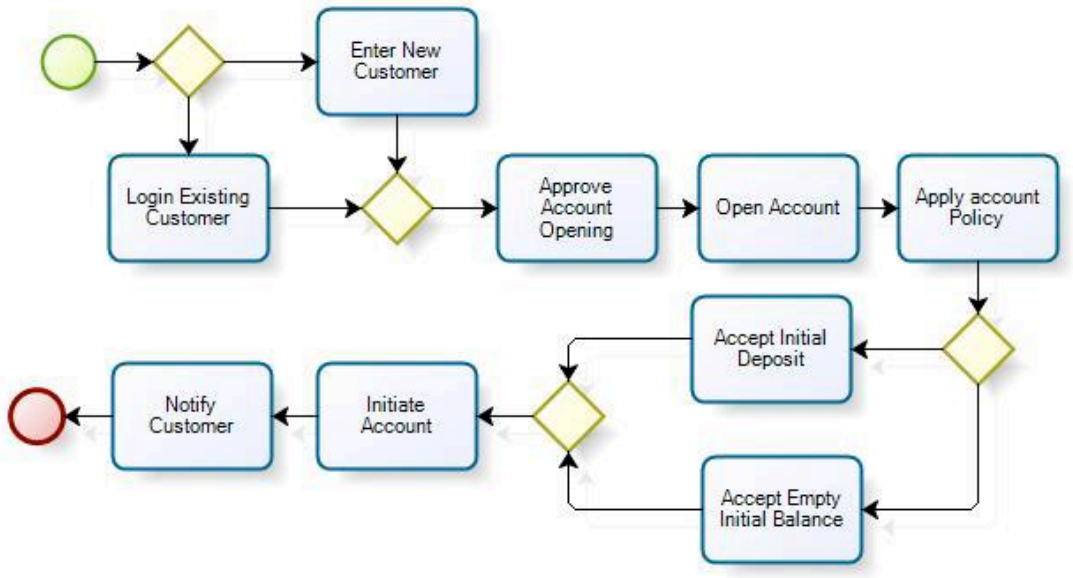

Figure 1: Example account-opening process

For a principles-based approach such as AML/CTF, the design of the internal controls typically reflects the *risk appetite* of the organization. Effective risk management begins with a clear understanding of an organization's appetite for risk and is essentially the process of identifying vulnerabilities and threats to the organization in achieving its business objectives. When establishing and implementing its system of risk management, a company will consider a number of risks such as financial reporting risks (the risk of a material error in the financial statements), operational, environmental, sustainability, strategic, external, ethical conduct, reputation or brand, technological, product or service quality, and human capital, as well as risks of noncompliance (ASX, 2006).

In order to handle the risk, the organization may choose one or more well-known strategies such as *avoid risk*, for example, if possible, choose not to implement processes and/or remove the source of the risk; *mitigate risk*, for example, define and implement controls; *transfer risk*, for example, share or outsource risk (insurance); and/or *accept risk*, for example, formally acknowledge existence of risk and monitor it.

The approach to risk management has a profound impact on how an organization would design and implement internal controls in response to compliance obligations. *Controls management* thus becomes a balancing act between compliance obligations, business objectives, and risks.

In the next section, we present a methodology for compliance management that aims to provide a means of aligning business and control objectives by using BPM and related technologies as drivers.

3 Methodology for Compliance Management

Previously, we have argued that *compliance by design* is a preferred approach for compliance management due to its preventative focus. In light of the heavy social, economic, and environmental costs of noncompliance, a priori embedding of requisite checks and triggers into the enterprise applications is clearly desirable but also extremely difficult, given that the business and technology landscape of today's organizations is disparate and distributed.

BPM is recognized as a means to enforce corporate policy. Regulatory mandates also provide policies and guidelines for business practice. One may argue why a separate requirements modeling facility is required to capture compliance requirements for business processes. We identify the following reasons against this argument:

Firstly, the source of these two objectives will be distinct, both from an ownership and governance perspective, as well as from a timeline perspective. Whereas businesses can be expected to have some form of business objectives, control objectives can be dictated by external sources and at different times.

Secondly, the two have differing concerns, namely, business objectives and control objectives. Thus, the use of business process languages to model control objectives may not provide a conceptually faithful representation. Compliance is in essence a normative notion, and thus control objectives are fundamentally descriptive, that is, indicating *what* needs to be done (in order to comply). Business process specifications are fundamentally prescriptive in nature, that is, detailing *how* business activity should take place. There is evidence of some developments toward descriptive approaches for BPM, but these works were predominantly focused on achieving flexibility in business process execution (e.g., Pesic and van der Aalst, 2006; Sadiq et al., 2005).

Thirdly, there is likelihood of conflicts, inconsistencies, and redundancies within the two specifications. The intersection of the two, thus, needs to be carefully studied.

In summary, we present in Fig. 2, the interconnect between process management and controls management. The two are formulated by different stakeholders and have different lifecycles. The design of control will impact the way a business process is executed. On the other hand, a (re)design of a business process causes an update of the risk assessment, which may lead to a new/updated set of controls.

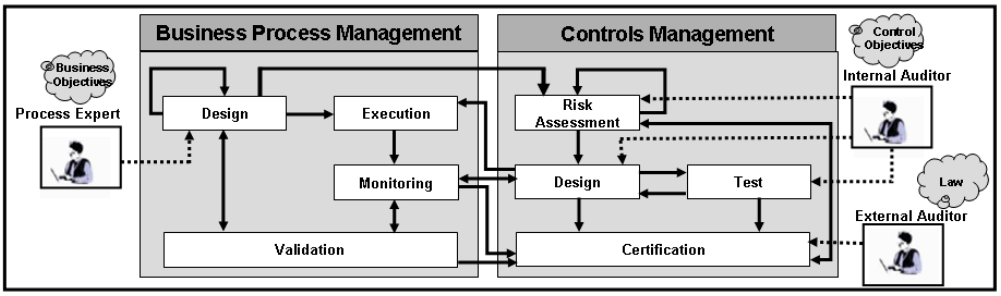

Figure 2: Interconnection of process management and controls management

Additionally, business process monitoring will assess the design of internal controls and

serve as an input to internal controls certification.

Given the scale and diversity of compliance requirements and additionally given the fact that these requirements may frequently change, business process compliance is indeed a large and complex problem area with several challenges. Given further that business and control objectives are (or should be) designed separately, but must converge at some point, we present below a list of essential requirements and where relevant corresponding techniques and methods that need to be met/ developed in order to tackle this overall problem.

3.1 Control Directory Management

Regulations and other compliance directives are complex and vague and require interpretation. Often in legalese, these mandates need to be translated by experts. For example, the COSO framework (COSO, 1994) is recognized by regulatory bodies as a de facto standard for realizing controls for financial reporting. A company-specific interpretation results in the following (textual) information being created:

$$\langle \textit{control objective}, \textit{risk}, \textit{internal control} \rangle$$

For example

Control objective:	Prevent unauthorized use of purchase order process;
Risk:	Unauthorized creation of purchase orders and payments to nonexisting suppliers;
Internal Control:	The creation and approval of purchase orders must be undertaken by two separate purchase officers.

The above example is typical of the well-known segregation-of-duty constraint (one individual does not participate in more than one key trading or operational function) mandated by Sarbanes-Oxley 404.

However, business will typically deal with a number of regulations/standards at one time. Thus there is a need to provide a structured means of managing the various interpretations within regional industry sector and organizational contexts.

We identify this as a need for a *controls directory*. Control directory management could be supported by database technology, and/or could present some interesting content management challenges, but will be an essential component in the overall solution. There is some evidence in industry reports that solution vendors are producing repositories of control objectives (and associated parameters) against the major regulations, see, for example, SAP GRC Repository and SAI Global GRC Knowledge and Information Services. Keeping abreast of frequently changing regulations is a clear challenge in the maintenance of such knowledge bases.

3.2 Ontological Alignment

Due to the diversity of stakeholders in compliance management initiatives, any effort towards providing compliance management solutions demands a common understanding of compliance management concepts and practice. For example, interpretation of regulations from legal

/financial experts comes in the form of textual descriptions (see example in the previous section). Establishing an agreement on terms and usage between these descriptions and the business processes and constituent activities/transactions is a difficult but essential aspect of the overall methodology.

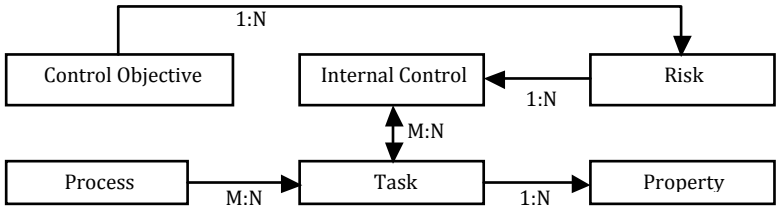

Figure 3: Relationships between process modeling and control modeling concepts

In Fig. 3, we present the relationships between the basic process modeling and control modeling concepts. Clearly, the relationship between process task and internal controls is much deeper than shown, as it would require alignment between embedded concepts, for example, task identification, particular data items, roles and performers, etc. However, it is evident that several controls may be applicable on a task, and one control may impact on multiple tasks as well.

What tools and techniques are utilized to provide an effective alignment between the two conceptual spaces is an important question at hand. Some recent work (Abdullah et al., 2012) reports on research undertaken to develop an ontology to create a shared conceptualization of the compliance management domain, namely CoMOn (Compliance Management Ontology). The ontology concepts are extracted from interviews and surveys of compliance management experts and practitioners, and refined through synthesis with leading academic literature related to compliance management. A semiotic framework has been utilized to conduct a rigorous evaluation of CoMOn through a series of eight case studies spanning a number of industry sectors. The consensus achieved through the evaluation positions CoMOn as a comprehensive domain ontology for Compliance Management.

3.3 Modelling Controls

The motivation to model controls is multifaceted. Firstly, a generic requirements modeling framework for compliance by design will provide a substantial improvement over current after-the-fact detection approaches. Secondly, it will allow for an analysis of compliance rules, thereby providing the ability to discover hidden dependencies, and view in holistic context, while maintaining a comprehensible working space. Thirdly, a precise and unambiguous (formal) specification will facilitate the systematic enrichment of business processes with control objectives.

A fundamental question in this regard is the *appropriate formalism* to undertake the task. In the next section, we will deliberate further on this question and provide a discussion of complementary approaches in this regard.

Note, however, that modeling controls in a precise and unambiguous manner is a necessary first step, but cannot completely address compliance by design methodology. Process model enrichment as explained in the next section, constitutes a second essential step.

3.4 Process Model Enrichment

In this context, we use the term process model enrichment as the ability to enhance enterprise models (business processes) with compliance requirements. This can be provided as process annotation. Process annotations have been proposed by a number of researchers, for example, the notion of control tags (Sadiq et al., 2007), integrating risks on EPCs (zur Mühlen and Rosemann, 2005), and semantic annotations (Governatori, Hoffmann et al., 2009). The resultant visualization of controls on the process model facilitates a better understanding of the interaction between the two specifications for both stakeholders (process owners as well as compliance officers).

Consider, for example, the account-opening process presented in Figure 1 An annotation at the activity "Enter New Customer" to indicate the need for "scanning of all new customer accounts against blocked entity data-sets" will assist in identifying the obligations relevant to AML/CTF. Figure 4 depicts a fragment of the process model presented in Figure 1 and shows an example of process annotation and resultant process redesign.

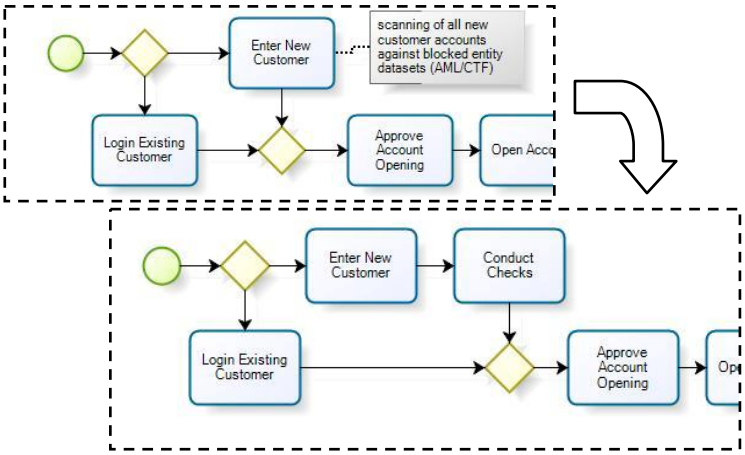

Figure 4: Example process annotation and resultant redesign

However, the visualization is only a first step. The new checks introduced within the process model can in turn be used to analyze the model for measures such as *compliance degree* (Lu et al., 2007), which can provide a quantification of the effort required to achieve a compliant process model. Eventually, process models may need to be modified to include the compliance requirements.

In large organizations, the process portfolio may consist of hundreds of process models that may span several business units. A diagnostic facility (Governatori, Hoffmann et al., 2009) can empower the organizations to undertake a compliance assessment at a large scale, and then

continue with compliance enforcement based on the measured compliance degree (or gap) and associated risks.

Sections 3.1–4.2 as presented above are focused on providing *design time* support for compliance management. Although model-driven enforcement and monitoring is a main objective of the presented methodology, it is not always possible to achieve. Below, we present a brief summary of issues and techniques for *run time* support for compliance management.

3.5 Compliance Enforcement

Enforcement of controls is a key component in the overall methodology. Given that the technology landscape of today's organizations is highly diverse and disparate, translation of designed internal controls onto the IT infrastructure, and subsequently, into business transactions is clearly a significant challenge. A number of complementary technologies can be identified in this regard.

- Records management (e.g., incident logging, data retention systems, etc.)
- Integration technologies (e.g., enterprise application integration, master data management)
- Testing/simulation (e.g., what-if scenario analysis)
- Control automation (e.g., rule engines)

Model-driven business process execution (as envisaged in the ideal BPM vision) is of course a candidate in the above, and arguably provides the most effective means to enforcement of compliance-related controls. Unfortunately, the current state of enterprise systems does not reflect the ideal BPM vision, and hence, compliance enforcement is provided through a variety of tools and technologies.

3.6 Compliance Monitoring

The support provided in the design of compliant processes through process annotation and analysis and resultant process changes can eventually lead to a *model-driven enforcement of compliance controls* (where process management systems are in place). However, it is naïve to assume that all organizations have the complete implementation of the BPM life cycle, and hence the process models and underlying applications may be disconnected. In this case, it is important to provide support for compliance through run-time monitoring. This has been the agenda for several vendors in this space targeting the so-called-automated detection, described earlier. In general, event monitoring is a well studied research topic (see, e.g., `www.complexevents.com`) and, although has not been widely/explicitly associated with the compliance issue, notably excepting Giblin et al. (2006), its usage in fraud detection and security is closely related.

Although, this chapter is primarily targeted at approaches conducive to achieving compliance by design by adopting a preventative approach facilitated by business process models, several works on formal modeling of control objectives (Governatori and Rotolo, 2006, 2010) have taken into account the violations and resultant reparation policies that may surface at runtime. Similarly, in (Conforti et al., 2011) a real-time risk detection method for business processes has been proposed.

SOURCES (Journals)	**TOTAL**	**Relevant Articles**	%	**SOURCES** (Conferences)	**TOTAL**	**Relevant Articles**	%
CAIS	659	16	2.4	BPM	189	7	3.7
BPMJ	336	5	1.5	ACIS	906	28	3.1
JAIS	158	2	1.3	CAiSE	346	9	2.6
JI&M	502	4	0.8	ICIS	959	14	1.5
CACM	2178	17	0.8	PACIS	1025	14	1.4
JISR	199	1	0.5	AMCIS	3822	46	1.2
EJIS	382	2	0.5	HICSS	4517	49	1.1
MISQ	281	1	0.4	ECIS	1489	17	1.1
				ER	400	2	0.5

Table 1: Sources and Frequency of Publication

4 State of the Art

Governance, risk, and compliance (GRC) is an emerging area of research that holds challenges for various communities including information systems; business software development; legal, cultural, and behavioral studies; and corporate governance. In (Abdullah, Indulska et al., 2009), GRC challenges emerging from industry have been related to existing activity in IS research between 2001–2010). Table 1 presents a snap shot of research contributions from notable IS journal and conferences. See (Abdullah, Indulska et al., 2009) for more details on methodology and results of the literature review)

As expected in an emerging research domain, the majority of the publications were found to be in the case study or exploratory paper category – 188 (81%) of the articles are case study/exploratory articles and 40 (17.2%) are solution articles. However, there are four (1.7%) articles that matched both types of articles. The results suggest that research on GRC solutions has being initiated but remains still in the early exploratory stages.

In this chapter, we have focused on compliance management from an information systems perspective, in particular the modeling and analysis of compliance requirements. In this section, we report on the contributions from research and academia in the area of compliance management. The primary focus of the discussion is on preventative approaches to compliance or those that facilitate compliance by design, and hence the discussion is structured around issues relating to Sections 4.1–4.2, that is *Modelling Controls* and *Process Model Enrichment*. A case study supported by a prototype implementation of these two phases of the methodology is subsequently presented in Section 5.

4.1 Modelling Controls

Both process modeling and modeling of normative requirements are well-studied fields independently, but until recently, the interactions between the two have been largely ignored (Desai, Mallya et al., 2005; Padmanabhan et al., 2006). In particular, zur Mühlen, Indulska et al. (2007) provide a valuable representational analysis to understand the synergies between process modeling and rule modeling. Similarly Cheng et al. (2011) provide a basic framework

for business process and rule integration using BPMN and SBVR as examples. It is obvious that the modeling of controls will be undertaken as rules, although the question of appropriate formalism is still under study. A plethora of proposals exist both in the research community on formal modeling of rules and in the commercial arena through business rule management systems.

Historically, formal modeling of normative systems has focused on how to capture the logical properties of the notions of the normative concepts (e.g., obligations, prohibitions, permissions, violations, etc.) and how these relate to the entities in an organization and to the activities to be performed. Deontic logic is the branch of logic that studies normative concepts such as obligations, permissions, prohibitions, and related notions. Standard deontic logic (SDL) is the starting point for logical investigation of the basic normative notions and offers a very idealized and abstract conceptual representation of these notions, but at the same time, it suffers from several drawbacks, given its high level of abstraction (Sartor, 2005). Over the years, many different deontic logics have been proposed to capture the different intuitions behind these normative notions and to overcome drawbacks and limitations of SDL. One of the main limitations in this context is its inability to reason with violations and the obligations arising in response to violations (Carmo and Jones, 2002). Very often, normative statements pertinent to business processes, and in particular contracts, specify conditions about when other conditions in the document have not been fulfilled; that is, when some (contractual) clauses have been violated. Hence, any formal representation to be conceptually faithful has to be able to deal with these kinds of situations.

As we have discussed before, compliance is a relationship between two sets of specifications: the normative specifications that prescribe what a business has to do and the process modeling specification describing how a business performs its activities. Accordingly, to properly verify that a process/procedure complies with the norms regulating the particular business, one has to provide conceptually sound representations of the process on one side and the norms on the other, and then check the alignment of the formal specifications of the process and the formal specifications for the norms.

In the following paragarph, we present an account of the various proposals for formal modeling regulations in the context of business process compliance. Governatori (2005); Governatori, Milosevic et al. (2006); Governatori and Rotolo (2010) have proposed FCL (formal contract language) as a candidate for control modeling, which has proved effective due to its ability to reason with violations and exceptions. FCL has been obtained from the combination of defeasible logic (for the efficient and natural treatment of exceptions, which are a common feature in normative reasoning) (Antoniou et al., 2001) and a deontic logic of violations (Governatori and Rotolo, 2006). In FCL a norm is represented by a rule, where a rule is an expression of the form

$$r\colon a_1, \ldots, a_n \Rightarrow c$$

where r is the name of the rule (unique for each rule) $a_1, \ldots, a_n$ are the conditions of applicability of the norm/rule or *premises* (represented by proposition in the logic) and c, the *conclusion* of the rule, is the *normative effect* of the norm/rule (again c is an expression or proposition of the logic).

The propositions of the logic are built from a finite set of atomic propositions, and the

following operators: ¬ (negation), [O] (obligation), [P] (permission), ⊗ (violation/reparation). The formation rules are as follows:

- Every atomic proposition is a proposition;
- If p is an atomic proposition, then $\neg p$ is a proposition;
- If p is a proposition, then $[O]p$ is an obligation proposition and $[P]p$ is a permission proposition. Obligation propositions and permission propositions are deontic propositions;
- If $p_1, \ldots, p_n$ are obligation propositions and q is a deontic proposition, then $p_1 \otimes \cdots \otimes p_n \otimes q$ is a reparation chain.

A simple proposition corresponds to a factual statement. The deontic operators are then indexed by the subject of the normative position corresponding to the operator. Thus $[O_s]$*Send Invoice* means that the supplier s has the obligation to send the invoice to the purchaser, and $[P_p]$*Charge Penalty* means that the purchaser p is entitled (permitted) to charge a penalty to the supplier. For obligations FCL supports both maintenance obligations (e.g., "the supplier must keep confidential the personal information provided by the customer") and achievement obligations (e.g. "a customer has to pay for the services received from the provider"), and for achievement obligations both pre-emptive and non-pre-emptive obligations – see (Governatori and Rotolo, 2010) for full details. A reparation chain, for example:

$$[O_s]\mathit{ProvidesGoodsTimely} \otimes [O_s]\mathit{OfferDiscount} \otimes [P_p]\mathit{ChargePenalty}$$

captures obligations and normative positions arising in response to violations of obligation. Thus the expression above means that the suppliers have the obligation to send the goods in a timely manner, but in case they do not comply with this (i.e., they violate the obligation do so) then they have the "secondary" obligation to offer a discount for the merchandise, and in case that they fail to fulfill this obligation (i. e., we have a violation of the possible reparation of the "primary" obligation), then, finally, the purchaser can charge the supplier with the penalty.

As usual in normative reasoning, there are two types of rules: definitional rules and normative rules. A definitional rule gives the conditions that assert a factual statement or to introduce new terms. A normative rule allows us to conclude obligations, permissions and prohibitions[3]. According to the above distinction in definitional rules, the conclusion is a proposition, and in normative rules, the conclusion is either a deontic proposition or a reparation chain. In both cases, the premises are propositions and deontic propositions, but not reparation chains. For example the definitional rule

$$\mathit{Customer}(x), \mathit{Spending}(x) > 1000 \Rightarrow \mathit{PremiumCustomer}(x)$$

specifies that, typically, a premium customer is a customer who has spent over 1000 dollars; while the following is an example of a normative rule:

$$\mathit{Restaurant}, [P]\mathit{SellAlcohol} \Rightarrow [OM]\mathit{ShowLicense}[OAPNP]\mathit{PayFine}.$$

The rule above means that if a restaurant has a license to sell alcohol (i.e., it is permitted to sell it, $[P]$*SellAlcohol*), then it has a maintenance obligation to expose the license ($[OM]$*ShowLicense*),

[3] Note that obligations allow us to capture prohibitions; a prohibition is an obligation plus negation, for example the prohibition to smoke can be understood as the obligation not to smoke.

if it does not then it has to pay the fine ([OAPNP]*PayFine*). The obligation to pay the fine is non-pre-emptive (this means it cannot be paid before the violation). Notice that FCL allows deontic expression (but not reparation chains) to appear in the body of rules.

FCL offers two reasoning modules: (1) a normalizer to make explicit rules that can be derived from explicitly given rules by merging their normative conclusions, to remove redundancy and identify conflicts rules, and (2) an inference engine to derive conclusions given some propositions as input.

Finally, FCL is agnostic about the nature of the literals it uses. They can represent tasks (activities executed in a process) or propositions representing state variables. For full description of FCL and its feature see (Governatori, 2005; Governatori and Rotolo, 2010).

There have been some other notable contributions from research on the matter of control modeling. Goedertier and Vanthienen (2006) present a logical language PENELOPE, which provides the ability to verify temporal constraints arising from compliance requirements on effected business processes. Küster et al. (2007) provide a method to check compliance between object life cycles that provide reference models for data artifacts, for example, insurance claims and business process models. Giblin et al. (2006) provide temporal rule patterns for regulatory policies, although the objective of this work is to facilitate event monitoring rather than the usage of the patterns for support of design time activities. Furthermore, Agrawal et al. (2006) have presented a workflow architecture for supporting Sarbanes–Oxley internal controls, which includes functions such as workflow modeling, active enforcement, workflow auditing, as well as anomaly detection.

There has been some complementary work in the analysis of formal models representing normative notions. For example, Farrell et al. (2005) study the performance of business contract on the basis of their formal representation. Desai, Narendra et al. (2008) seek to provide support for assessing the correctness of business contracts represented formally through a set of commitments. The reasoning is based on value of various states of commitment as perceived by cooperative agents. Research on closely related issues has also been carried out in the field of autonomous agents (Alberti et al., 2006).

4.2 Process Model Enrichment

As discussed previously, modeling the controls is only the first step toward compliance by design. The second essential step is the enrichment of process models with compliance requirements (i.e., the modeled controls). Clearly, this cannot take place without a formal controls model (as proposed by above-mentioned works), or at least some machine-readable specification of the controls.

There have recently been some efforts toward support for business process modeling against compliance requirements. In particular, the works of zur Mühlen and Rosemann (2005) and Neiger et al. (2006) provide an appealing method for integrating risks in business processes. The proposed technique for "risk-aware" business process models is developed for EPCs (event process chains) using an extended notation. Sadiq et al. (2007) propose an approach based on control tags to visualize internal controls on process models. Liu et al. (2007) takes a similar approach of annotating and checking process models against compliance rules, although the visual rule language, namely BPSL, is general purpose and does not directly address the notions

representing compliance requirements.

4.3 Summary

Although this chapter has primarily focused on preventative approaches to compliance, it is important to identify the role of detective approaches as well, where a wide range of supporting technologies are present. These include several commercial solutions such as business activity monitoring, BI, etc. Noteworthy in research literature with respect to compliance monitoring is the synergy with process mining techniques (van der Aalst et al., 2003; van Dongen et al., 2005) that provide the capability to discover run-time process behavior (and deviations) and can thereby assist in detection of compliance violations.

In terms of the compliance services and solutions, a number of compliance service/solution providers are currently available, including large consulting firms providing business services and advisory as well as software vendors. Software services are emerging from large corporations with products such as IBM Lotus workplace for business controls and reporting, Microsoft Office Solutions Accelerator for Sarbanes–Oxley, SAP GRC Solution, as well as niche vendors such as OpenPages, Paisley Consulting, Qumas Inc., and several others (Caldwell and Eid, 2008).

Software solutions and tools for compliance are typically found under the umbrella of other technologies such as BI, business rules management, etc. As such, compliance vendors are not easily identified directly. Further, while many vendors provide sophisticated functionality of some aspect of the overall end-to-end methodology (as presented in Section 3), these solutions are of a piecemeal nature, for example, a business controls and reporting tool designed to help users manage processes, controls, and information, subject to Sarbanes-404.

5 Case Study

In this section we first introduce the architecture for a business process compliance checker based on the methodology developed by Governatori and Sadiq (2009) and presented in this chapter. As we have already discussed that to check whether a business process is compliant with a relevant regulation, we need an annotated business process model (process model enrichment) and the formal representation (modeling controls) of the regulation. The annotations are attached to the tasks of the process, and it can be used to record the data, resources and other information related to the single tasks in a process. For the formal representation of the regulation we use FCL (Governatori, 2005; Governatori and Rotolo, 2010) as briefly introduced in the previous section.

Compliance is not just about the tasks to be executed in a process but also on what the tasks do, the way they change the data and the state of artifacts related to the process, and the resources linked to the process. Accordingly, process models must be enriched with such information. Sadiq et al. (2007) proposed to enrich process models with semantic annotations. Each task in a process model can have attached to it a set of semantic annotations. In our approach the semantic annotations are literals in the language of FCL, representing the effects of the tasks. The approach can be used to model business process data compliance (Hashmi et al., 2012).

Figure 5 depicts the logical outline of the architecture. Given an annotated process and the formalisation of the relevant regulation, we can use the algorithms proposed by Governatori

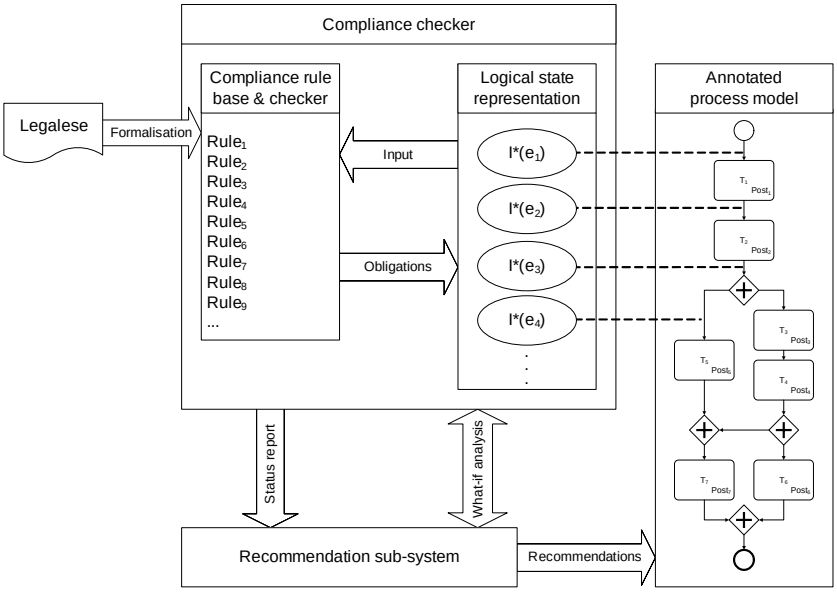

Figure 5: Architecture of Compliance Checker

and Rotolo (2008, 2010) to determine whether the annotated process model is compliant. The process runs as follows:

- Generate an execution trace of the process.
- Traverse the trace:
  - for each task in the trace, cumulate the effects of the task using an update semantics (i.e., if an effect in the current task conflicts with previous annotation, update using the effects of the current tasks).
  - use the set of cumulated effects to determine which obligations enter into force at the current tasks. This is done by a call to an FCL reasoner.
  - add the obligations obtained from the previous step to the set of obligations carried over from the previous task.
  - determine which obligations have been fulfilled, violated, or are pending; and if there are violated obligations check whether they have been compensated.
- repeat for all traces.

A process is *compliant* if and only if all traces are compliant (all obligations have been fulfilled or if violated they have been compensated). A process is *weakly compliant* if there is at least one trace that is compliant.

We now describe the implementation of a prototype, called BPCC based on the above architecture, which has been tested an evaluated with an industry scale real life case study, reported in (Governatori and Shek, 2012).[4]

[4]For more information about BPCC see `http://www.nicta.com.au/research/projects/bpc`.

BPCC is implemented on top of Eclipse. For the representation of process models, it uses the Eclipse Activiti BPMN 2.0 plugin, extended with features to allow users to add semantic annotations to the tasks in the process model. BPCC is process model agnostic, this means that while the current implementation is based on BPMN all BPCC needs is to have a description of the process and the annotations for each task. A module of BPCC take the description of the process and generates the execution traces corresponding to the process. After the traces are generated, it implements the algorithm outlined in the previous section, where it uses the SPINdle rule engine (Lam and Governatori, 2009) for the evaluation of the FCL rules. In case a process is not compliant (or if it is only weakly compliant) BPCC reports the traces, tasks, rules and obligations involved in the non compliance issues (see Figure 6).

BPCC was tested against the 2012 Australian Telecommunications Customers Protection Code (C628-2012). The code is effective from September 1st 2012. The code requires telecommunication operators to provide annual attestation of compliance with the code staring from April 1st 2013. The evaluation was carried out in May-June 2012. Specifically, the section of the code on complaint handling has been manually mapped to FCL. The section of the code contains approximately 100 commas, in addition to approximately 120 terms given in the Definitions and Interpretation section of the code. The mapping resulted in 176 FCL rules, containing 223 FCL (atomic) propositions, and 7 instances of the superiority relation. Of the 176 rules 33 were used to capture definitions of terms used in the remaining rules. Mapping the section of the code required all features of FCL: all types of obligations apart punctual obligations were used, reparation chains, permissions, defeasibility to easily capture exceptions, and obligations and permissions in the body of rules.

The evaluation was carried over in cooperation with an industry partner subject to the code. The industry partner did not have formalised business processes. Thus, we worked with domain experts from the industry partner (who had not been previously exposed to BPM technology, but who were familiar with the industry code) to draw process models for the activities covered by the code. The evaluation was carried out in two steps. In the first part we modelled the processes they were. BPCC was able to identify several areas where the existing processes were not compliant with the new code. In some cases the industry partner was already aware of some of the areas requiring modifications of the existing processes. However, some of the compliance issues discovered by the tools were novel to the business analysts and were identified as genuine non-compliance issues that need to be resolved. In the second part of the experiment, the existing processes were modified to comply with the code based on the issues identified in the first phase. In addition a few new business process models required by the new code were designed. As result we generated and annotated 6 process models. 5 of the 6 models are limited in size and they can be checked for compliance in seconds. The largest process contains 41 tasks, 12 decision points, xor splits, (11 binary, 1 ternary). The shortest path in the model has 6 tasks, while the longest path consists of 33 tasks (with 2 loops), and the longest path without loop is 22 task long. The time taken to verify compliance for this process amounts approximately to 40 seconds on a MacBook Pro 2.2Ghz Intel Core i7 processor with 8GB of RAM (limited to 4GB in Eclipse).

A few other compliance prototypes have been proposed: MoBuCom (Maggi et al., 2011), Compass (Elgammal et al., 2012) and SeaFlows (Ly et al., 2012). MoBuCom and Compass are based on Linear Temporal Logic (LTL) and mostly address “structural compliance” (i.e., that

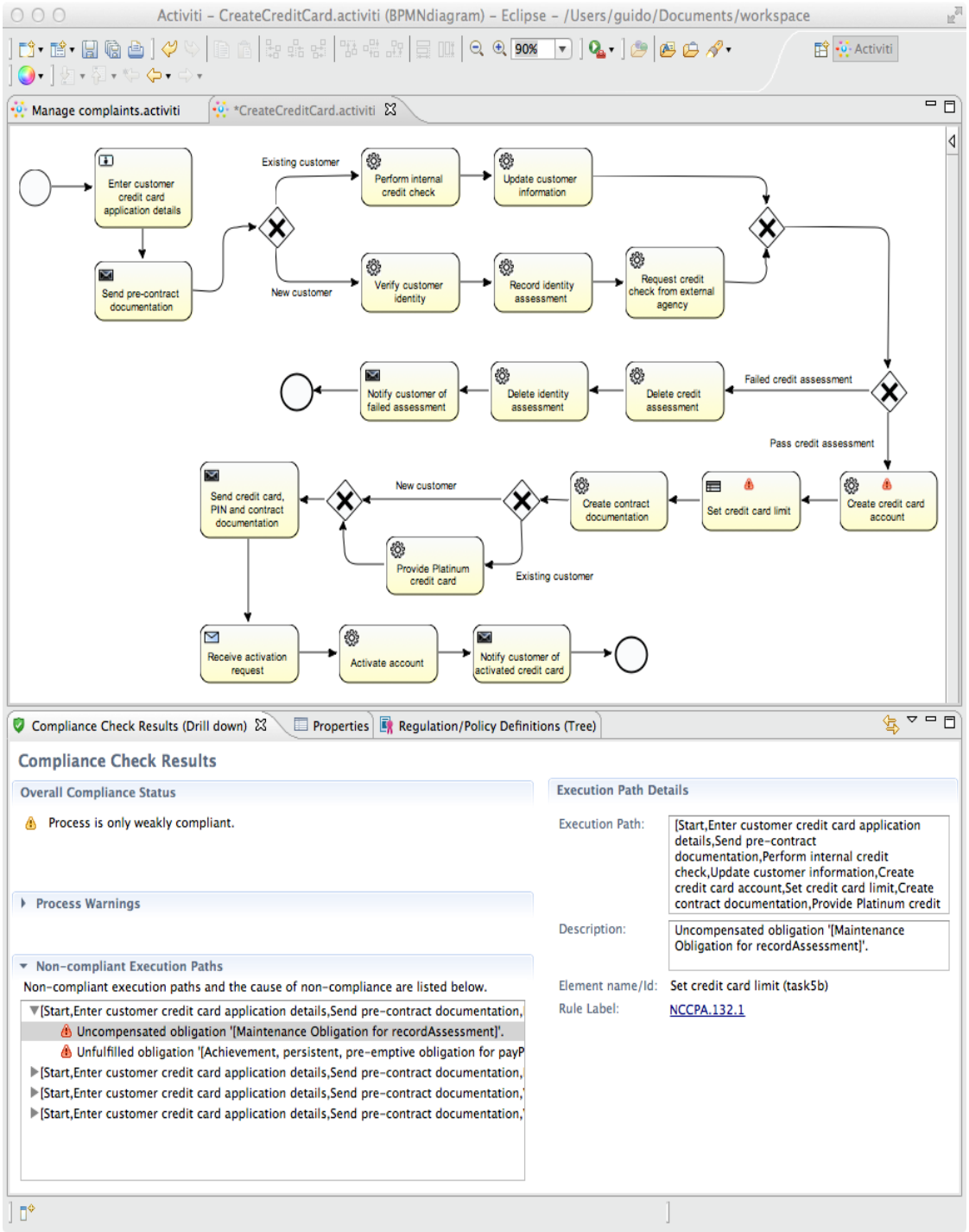

Figure 6: Example of non-compliant report in BPCC

the tasks are executed in the relative order defined by a constraint model). The use of LTL implies that the model on which these tools are based on is not conceptually relative to the legal domain, and thus fails to capture nuances of reasoning with normative constrains such as violations, different types of obligations, violations and their compensation. For example, obligations are represented by temporal operators. This raises the problem of how to represent the distinction between achievement and maintenance obligations. A possible solution is to use always for maintenance and sometimes for achievement, but this leaves no room for the concept of permission (the permission is dual of obligation, and always and sometimes are the dual of each other). In addition using temporal operators to model obligations makes it hard to capture data compliance (Hashmi et al., 2012), i.e., obligations that refer to literals in the same task. SeaFlow is based on first-order logic, and it is well know that first oder logic is not suitable to capture normative reasoning (Herrestad, 1991). On the other hand FCL and consequently BPCC comply with the guidelines set up in (Gordon et al., 2009) for a rule language suitable for representation of legal knowledge and legal reasoning.

6 Discussion and Outlook

As the importance of GRC grows for various industries, there is an evident need to provide supporting tools and methods to enable organizations seeking corporate social responsibility to achieve their objectives. The challenges that reside in this topic warrant systematic approaches that motivate and empower business users to achieve a high degree of compliance with regulations, standards, and corporate policies.

One of the biggest challenges facing the compliance industry is the measurement of adequacy of controls (KPMG Advisory, 2005), that is, achieving a balance between control and business objectives. This has been a driver of the research presented in this chapter. The methodology presented in Sect. 3 provides a systematic means of aligning business and control objectives. However, several open issues still remain. In (Abdullah et al., 2010), an industry driven research agenda for GRC has been presented, which highlights the main challenges and potential areas of future research. The agenda is aligned with the main message of this chapter and is summarized as below.

First and foremost, there is an urgent need for proper benchmarking studies to help address the challenge of high cost. Particularly for SMEs, there is high cost and great difficulty in measuring the adequacy of controls for principles based regulations where the onus is on the organization to design an appropriate compliance regimen. Benchmarking and best practice studies will allow improvement of controls effectiveness, a reduction of costs, and an improved potential to deal with resistance to change through demonstrating methods used by others. Such additional knowledge can further help alleviate the perception of legislation weaknesses in principles based regulations and consequently promote regulation acceptance.

In a related manner, there is also a need for investigation of process reference models relating to various regulations. A focus on the development of such reference models and the study of the impact of the use of such models in organizations (i.e. impact on compliance management spending, frequency of breaches, etc) is largely missing in Information Systems research. The development of proven reference models, however, may significantly lessen the

cost of compliance management in organizations.

The culture of compliance is ingrained in the daily rituals of each of the firm's employees, including senior management, who must learn to lead by example. There is a clear lack of Information Systems research on organisational behaviour. In particular we see a need for investigation of how IT and IS tools can be used to incentivize employees to 'do the right thing' and adapt their practices. There is also a need for the development of relevant IT and IS tools that can help facilitate employee training for compliance management, promote communication among staff and increase organizational capacity to manage its compliance knowledge base.

How the compliance (and risk) factor interrelates with the operations of business units is understudied, with only a small number of researchers working on the conceptualisation of compliance and risk requirements per se let alone their inter-relationships with business processes and business activities. A comprehensive and well-grounded conceptual model for compliance and risk is needed.

Further to the point above, tools and methods are needed to annotate, enhance, analyse and simulate business models with compliance and risk modeling elements. This will facilitate better coordination between an organization's compliance and business functions and help employees understand compliance value and business relevance.

Although reporting and monitoring tools of high sophistication are available, there is little development towards tools that provide specialized solutions in monitoring and analysing compliance related data (partly due the absence of generic conceptual models for GRC), thus causing big problems for organisations required to create evidence of compliance. Accordingly, we see a need for affordable IT and IS tools that facilitate compliance management self-audits and compliance monitoring activities in general. Furthermore, there is also a clear need for tools that facilitate the identification of non-compliance processes with respect to a given regulation.

Frequency of change, as well as inconsistency and overlaps in regulations is beyond the realm of IS research, studies to understand the impact of regulation changes (inconsistencies and overlaps) can promote better understanding of the cost of compliance and allow business to lobby for regulatory reform where needed. Multi disciplinary research is warranted in order to cover legal, business and IT aspects. From an Information Systems perspective, there is a need for solutions that can filter out updates that are not relevant to a given organization or industry sector, thus reducing the amount of information that the organization has to process in order to update or assess their compliance management initiatives.

In conclusion, future research endeavors in this area should strive toward compliance management frameworks that provide a close integration of the three perspectives, namely, preventative, detective, and corrective. Such a framework can allow organizations to better respond to the changing regulatory demands and also reap the benefits of process improvement.

Acknowledgements

NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program.

References

Abdullah, NS, M Indulska and S Sadiq (2009). "A study of compliance management in information systems research". In S Newell, EA Whitley, N Pouloudi, J Wareham, and L Mathiassen, eds. *17th European Conference on Information Systems* (ECIS 2009), pp. 1711–1721.

Abdullah, NS, S Sadiq and M Indulska (2010). "Emerging Challenges in Information Systems Research for Regulatory Compliance Management". In B Pernici, ed. *22nd International Conference on Advanced Information Systems Engineering* (CAiSE 2010). LNCS 6051, pp. 251–265. Springer, Heidelberg.

Abdullah, NS, S Sadiq and M Indulska (2012). "A Compliance Management Ontology: Developing Shared Understanding through Models". In J Ralyté, X Franch, S Brinkkemper, and S Wrycza, eds. *24th International Conference on Advanced Information Systems Engineering* (CAiSE 2012). LNCS 7328, pp. 429–444. Springer, Heidelberg.

Agrawal, R, CM Johnson, J Kiernan and F Leymann (2006). "Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology". In L Liu, A Reuter, KY Whang, and J Zhang, eds. *Proceedings of the 22nd International Conference on Data Engineering* (ICDE 2006), p. 92. IEEE Computer Society.

Alberti, M, M Gavanelli, E Lamma, F Chesani, P Mello and P Torroni (2006). "Compliance verification of agent interaction: a logic-based software tool". *Applied Artificial Intelligence*. 20(2-4): 133–157.

Alonso, G, P Dadam, and M Rosemann, eds. (2007). *5th International Conference on Business Process Management* (BPM 2007). LNCS 4714. Springer, Heidelberg.

Antoniou, G, D Billington, G Governatori and MJ Maher (2001). "Representation Results for Defeasible Logic". *ACM Transactions on Computational Logic*. 2(2): 255–287.

ASX (2006). *Australian securities exchange principles of good governance, recommendation 7.1*. URL: `http://www.asx.gov.au` (visited on 1st June 2008).

AUSTRAC (2006). *Australian transaction reports and analysis centre supervisory framework*. URL: `http://www.austrac.gov.au/files/supervisory_framework.pdf` (visited on 1st June 2008).

BPM Forum (2006). *CEE: the future. Building the compliance enabled enterprise*. Report produced by global fluency in partnership with: AXS-One, chief executive magazine and IT compliance institute.

Caldwell, F and T Eid (2008). *Magic quadrant for enterprise governance, risk and compliance platforms*. Gartner Research, G00158295, June 2008.

Carmo, J and AJ Jones (2002). "Deontic Logic and Contrary To Duties". In Gabbay, D, and F Guenther, eds. *Handbook of Philosophical Logic, 2nd Edition*. Vol. 8, pp. 265–343. Springer, Berlin.

Cheng, R, S Sadiq and M Indulska (2011). "Framework for Business Process and Rule Integration: A Case of BPMN and SBVR". In W Abramowicz, ed. *14th International Conference on Business Information Systems* (BIS 2011). LNBIP 87, pp. 13–24. Springer, Heidelberg.

Conforti, R, G Fortino, M La Rosa and AHM ter Hofstede (2011). "History-Aware, Real-Time Risk Detection in Business Processes". In R Meersman, TS Dillon, P Herrero, A Kumar, M Reichert, L Qing, BC Ooi, E Damiani, DC Schmidt, J White, M Hauswirth, P Hitzler, and MK Mohania, eds. *On the Move to Meaningful Internet Systems: OTM 2011 – Confederated*

International Conferences: CoopIS, DOA-SVI, and ODBASE 2011 (OTM Conferences). LNCS 7044, pp. 100–118. Springer, Heidelberg.

COSO (1994). *COSO: Internal Control, An Integrated Framework. The Committee of Sponsoring Organisations of the Treadway Commission.* The Committee of Sponsoring Organisations of the Treadway Commission.

Desai, N, AU Mallya, AK Chopra and MP Singh (2005). "Interaction Protocols as Design Abstractions for Business Processes". *IEEE Transactions on Software Engineering.* 31(12): 1015–1027.

Desai, N, NC Narendra and MP Singh (2008). "Checking correctness of business contracts via commitments". In L Padgham, DC Parkes, J Müller, and S Parsons, eds. *7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), pp. 787–794. IFAAMAS.

Eder, J, and S Dustdar, eds. (2006). *Business Process Management Workshops.* LNCS 4103. Springer, Heidelberg.

Elgammal, A, O Türetken and WJ van den Heuvel (2012). "Using Patterns for the Analysis and Resolution of Compliance Violations". *International Journal of Cooperative Information Systems.* 21(1): 31–54.

Farrell, ADH, MJ Sergot, M Sallé and C Bartolini (2005). "Using the event calculus for tracking the normative state of contracts". *International Journal of Cooperative Information Systems.* 14(2-3): 99–129.

Giblin, C, S Müller and B Pfitzmann (2006). *From Regulatory Policies to Event Monitoring Rules: Towards Model Driven Compliance Automation.* IBM Research Report. Zurich Research Laboratory. Oct. 2006.

Goedertier, S and J Vanthienen (2006). "Designing Compliant Business Processes with Obligations and Permissions". In Eder and Dustdar (2006), pp. 5–14.

Gordon, TF, G Governatori and A Rotolo (2009). "Rules and Norms: Requirements for Rule Interchange Languages in the Legal Domain". In Governatori, Hall and Paschke (2009), pp. 282–296.

Governatori, G (2005). "Representing Business Contracts in RuleML". *International Journal of Cooperative Information Systems.* 14(2-3): 181–216.

Governatori, G, J Hall, and A Paschke, eds. (2009). *International Symposium on Rule Interchange and Applications* (RuleML 2009). LNCS 5858. Springer, Heidelberg.

Governatori, G, J Hoffmann, SW Sadiq and I Weber (2009). "Detecting Regulatory Compliance for Business Process Models through Semantic Annotations". In D Ardagna, M Mecella, and J Yang, eds. *Business Process Management Workshops.* LNBIP 17, pp. 5–17. Springer, Heidelberg.

Governatori, G, Z Milosevic and S Sadiq (2006). "Compliance checking between business processes and business contracts". In PCK Hung, ed. *10th International Enterprise Distributed Object Computing Conference* (EDOC 2006), pp. 221–232. IEEE Computing Society.

Governatori, G and A Rotolo (2006). "Logic of Violations: A Gentzen System for Reasoning with Contrary-To-Duty Obligations". *Australasian Journal of Logic.* 4: 193–215.

Governatori, G and A Rotolo (2008). "An Algorithm for Business Process Compliance". In E Francesconi, G Sartor, and D Tiscornia, eds. *Legal Knowledge and Information Systems.* Frontieres in Artificial Intelligence and Applications 189, pp. 186–191. IOS Press.

Governatori, G and A Rotolo (2010). "A Conceptually Rich Model of Business Process Compliance". In S Link, and A Ghose, eds. *7th Asia-Pacific Conference on Conceptual Modelling* (APCCM 2010). CRPIT 110, pp. 3–12. ACS.

Governatori, G and S Sadiq (2009). "The Journey to Business Process Compliance". In Cardoso, J, and W van der Aalst, eds. *Handbook of Research on BPM*, pp. 426–454. IGI Global.

Governatori, G and S Shek (2012). "Rule Based Business Process Compliance". In *Proceedings of the RuleML2012@ECAI Challenge*. CEUR Workshop Proceedings 874, article 5.

Hagerty, J, J Hackbush, D Gaughan and S Jacobson (2008). *The governance, risk management, and compliance spending report, 2008–2009: Inside the $32B GRC Market.* AMR Research, Boston, USA, 25th Mar. 2008.

Hashmi, M, G Governatori and MT Wynn (2012). "Business Process Data Compliance". In A Bikakis, and A Giurca, eds. *6th International Symposium on Rules on the Web: Research and Applications* (RuleML 2012). LNCS 7438, pp. 32–46. Springer, Heidelberg.

Herrestad, H (1991). "Norms and formalization". In *Third International Conference on Artificial Intelligence and Law* (ICAIL 1991), pp. 175–184. ACM.

KPMG Advisory (2005). *The Compliance Journey: Balancing Risk and Controls with Business Improvement.*

Küster, JM, K Ryndina and H Gall (2007). "Generation of Business Process Models for Object Life Cycle Compliance". In Alonso, Dadam and Rosemann (2007), pp. 165–181.

Lam, HP and G Governatori (2009). "The Making of SPINdle". In Governatori, Hall and Paschke (2009), pp. 315–322.

Liu, Y, S Müller and K Xu (2007). "A static compliance-checking framework for business process models". *IBM Systems Journal.* 46(2): 335–362.

Lu, R, S Sadiq and G Governatori (2007). "Compliance Aware Business Process Design". In AHM ter Hofstede, B Benatallah, and HY Paik, eds. *Business Process Management Workshop.* LNCS 4928, pp. 120–131. Springer, Heidelberg.

Ly, LT, S Rinderle-Ma, K Göser and P Dadam (2012). "On enabling integrated process compliance with semantic constraints in process management systems - Requirements, challenges, solutions". *Information Systems Frontiers.* 14(2): 195–219.

Maggi, FM, M Montali, M Westergaard and WMP van der Aalst (2011). "9th International Conference on Business Process Management". In Rinderle-Ma, S, F Toumani, and K Wolf, eds. (BPM 2011). LNCS 6896, pp. 132–147. Springer, Heidelberg.

Neiger, D, L Churilov, M zur Muehlen and M Rosemann (2006). "Integrating risks in business process models with value focused process engineering". In J Ljungberg, and M Andersson, eds. *Proceedings of the Fourteenth European Conference on Information Systems* (ECIS 2006), pp. 1606–1615.

Padmanabhan, V, G Governatori, S Sadiq, RM Colomb and A Rotolo (2006). "Process Modelling: The Deontic Way". In M Stumptner, S Hartmann, and Y Kiyoki, eds. *Thirds Asia-Pacific Conference on Conceptual Modelling* (APCCM 2006), pp. 75–84. Australian Computer Science Communications.

Pesic, M and WMP van der Aalst (2006). "A Declarative Approach for Flexible Business Processes Management". In Eder and Dustdar (2006), pp. 169–180.

Sadiq, SW, ME Orlowska and W Sadiq (2005). "Specification and validation of process constraints for flexible workflows". *Information Systems.* 30(5): 349–378.

Sadiq, S, G Governatori and K Naimiri (2007). "Modelling of Control Objectives for Business Process Compliance". In Alonso, Dadam and Rosemann (2007), pp. 149–164.

Sartor, G (2005). *Legal Reasoning*. Dordrecht: Springer.

van der Aalst, WMP, BF van Dongen, J Herbst, L Maruster, G Schimm and AJMM Weijters (2003). "Workflow mining: A survey of issues and approaches". *Data and Knowledge Engineering*. 47(2): 237–267.

van Dongen, BF, AKA de Medeiros, HMW Verbeek, AJMM Weijters and WMP van der Aalst (2005). "The ProM Framework: A New Era in Process Mining Tool Support". In G Ciardo, and P Darondeau, eds. *26th International Conference Applications and Theory of Petri Nets 2005* (ICATPN 2005). LNCS 3536, pp. 444–454. Springer, Heidelberg.

zur Mühlen, M, M Indulska and G Kemp (2007). "Business Process and Business rule Modeling Languages for Compliance Management: A Representational Analysis". In *ER 2007: Tutorials, Poster, Panels, and Industrial Contribution*. CRPIT 83, pp. 127–132.

zur Mühlen, M and M Rosemann (2005). "Integrating Risks in Business Process Models". In *Proceedings of 16th Australasian Conference on Information Systems*.