A Methodological Framework for Aligning Business Processes and Regulatory Compliance

Shazia Sadiq

School of Information Technology and Electrical Engineering,
The University of Queensland, St Lucia QLD 4072
Australia
shazia@itee.uq.edu.au

Guido Governatori

NICTA, Queensland Research Laboratory, Australia
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 in over $32billion in 2008 0(Hagerty, Hackbush, Gaughan & Jacobson, 2008). The boost in business investment is primarily a consequence of regulatory mandates that emerged as a result of events that led to some of the largest scandals in corporate history such as Enron, WorldCom (USA), HIH (Australia) and Societe 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 said they expected to reap business benefits from improving their compliance regimens.

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

Corrective measures can be undertaken due to 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 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 towards 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, Governatori & Namiri, 2007). That is, compliance should be embedded into the business practice, rather than seen as a distinct activity. In particular, we argue that a *compliance by design* approach that capitalizes on 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, 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 detailed discussion on state of the art in compliance management services and solutions covering contributions from both academia as well as industry. The analysis of current solutions indicates that a process driven ap-

proach to compliance management may be the most effective way to address this complex problem. The chapter concludes with a discussion on open questions and challenges towards 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:

- customer due diligence (identification, verification of identity and ongoing monitoring of transactions)
- reporting (suspicious matters, threshold transactions and international funds transfer instructions)
- record keeping, and
- 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 Figure 1. An internal control may mandate the "scanning of all new customer accounts against blocked entity datasets" in response to the obligation to provide customer due diligence during the account opening process. This would require an additional check to be conducted after entering new customer information.

[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)

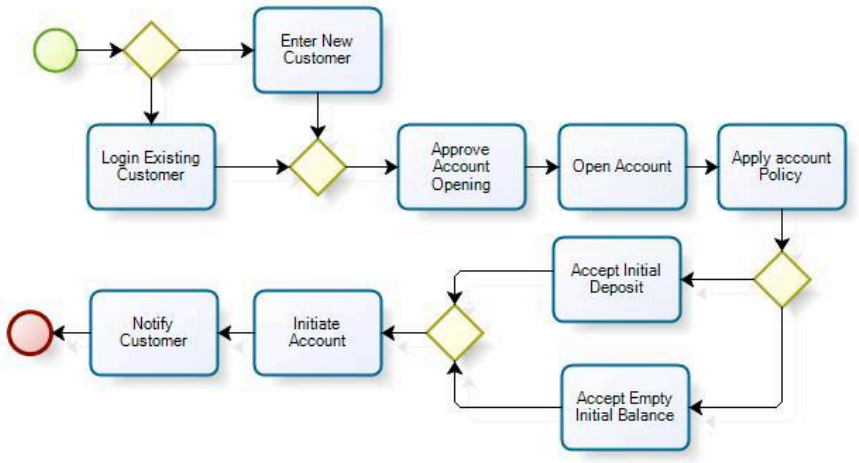

Fig. 1. Example Account Opening Process

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 organisation's appetite for risk and is essentially the process of identifying vulnerabilities and threats to the organisation 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 non-compliance (ASX, 2006).

In order to handle the risk, the organization may choose one or more of well known strategies such as: Avoid Risk e.g., if possible, choose not to implement processes and/or remove the source of the risk; Mitigate Risk e.g., define and implement controls; Transfer Risk e.g., share or outsource risk (insurance); and/or Accept Risk e.g., 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 business process management and related technologies, as a driver.

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 socio, economic and environmental costs of non-compliance, 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.

Business process management 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. Where as 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, i.e. indicating *what* needs to be done (in order to comply). Business process specifications are fundamentally prescriptive in nature, i.e. detailing *how* business activity should take place. There is evidence of some developments towards descriptive approaches for BPM, but these works were predominantly focused on achieving flexibility in business process execution, see e.g. (Pesic & van der Aalst, 2006), (Sadiq, Sadiq & Orlowska, 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 Figure 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 on 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. Additionally, business process monitoring will assess the design of internal controls and serve as an input to internal controls certification.

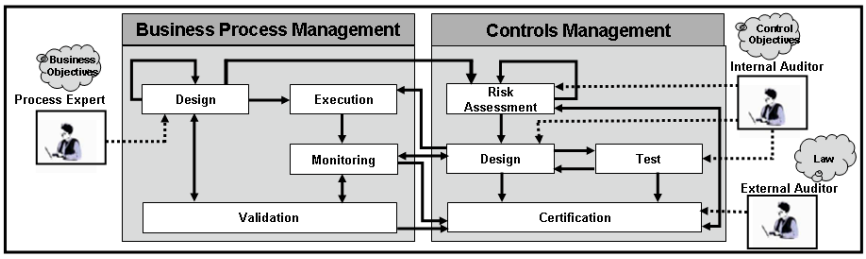

Fig. 2. Interconnect of Process Management and Controls Management

Given the scale and diversity of compliance requirements and additionally 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, 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:

<control objective, risk, internal control>

For example:

Control objective:	*prevent unauthorized use of purchase order process*
Risk:	*unauthorized creation of purchase orders and payments to non-existing 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 e.g. SAP GRC Repository, 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

Interpretation of regulations from legal /financial experts comes in the form of textual descriptions (see example in section above). 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.

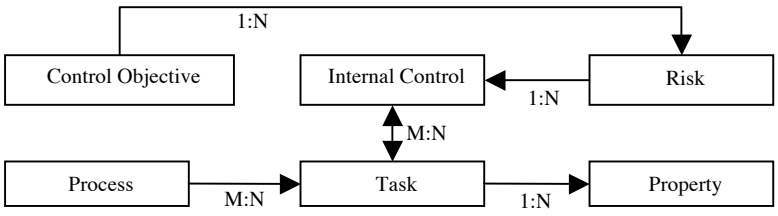

Fig. 3. Relationships between Process Modeling and Control Modeling Concepts

In the 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 e.g. 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 not the focus of this paper, but none the less an important question at hand.

3.3 Modeling 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 thus 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 the regard.

Note however, that modeling controls is 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 in a number of researchers, for example the notion of control tags in (Sadiq, Governatori &Namiri, 2007), integrating risks on EPCs (zur Muehlen & Rosemann, 2005), and semantic annotations (Governatori, Hoffmann, Sadiq, & Weber, 2008). 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 datasets" 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

However, the visualization is only a first step. The new checks introduced within the process model, can in turn be used to analyse the model for measures such as *compliance degree* (Lu, Sadiq & Governatori, 2008),

that 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.

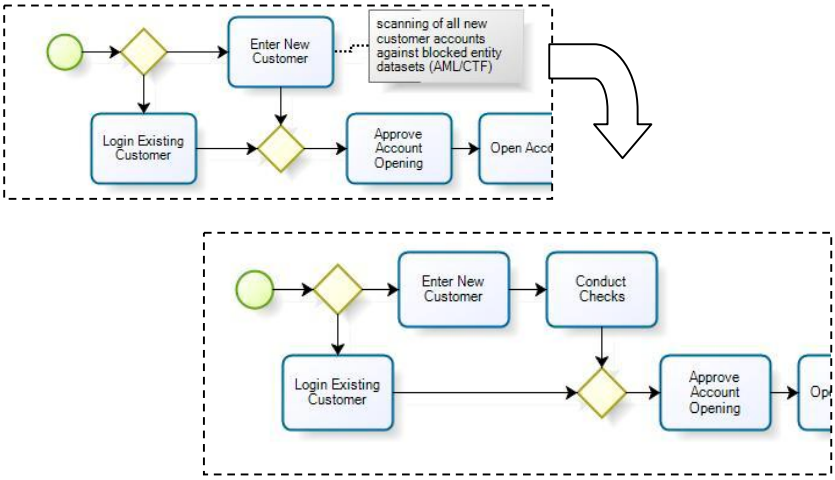

Fig. 4. Process Annotation and Resultant Re-design

In large organizations, the process portfolio may consist of 100s of process models that may span several business units. A diagnostic facility (Governatori, Hoffmann, Sadiq & Weber, 2008) 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.

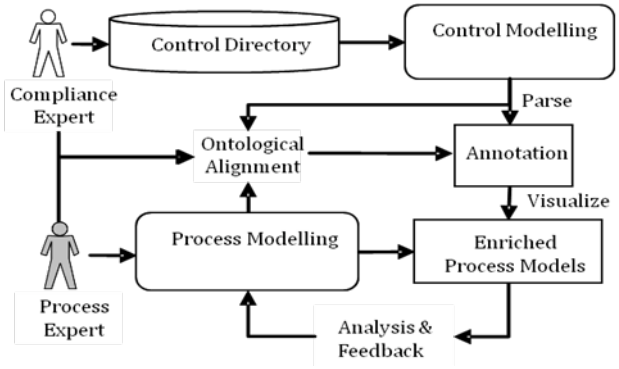

Fig. 5. Summary of Design Time Support in the Methodology

The methodology as presented so far can be summarized in figure 5. Note however, that the sections 3.1 – 3.4 as presented above are focussed 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 such as.

- 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 providing 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 lifecycle, and hence the process models and underlying applications may be disconnected. In this case, it is important to provide support for compli-

ance 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, Muller & Pfitzmann, 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 & Rotolo, 2006) have taken into account the violations and resultant reparation policies that may surface at runtime.

4 State of the Art

Governance, risk and compliance (GRC) is an emerging area of research which holds challenges for various communities including information systems, business software development, legal, cultural, & behavioral studies and corporate governance.

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 as well as industry solutions 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 **compliance modeling** specifically issues relating to sections 3.3 – 3.4.

4.1 Modeling Controls

Both process modeling as well as modeling of normative requirements are well studied fields independently, but until recently the interactions between the two have been largely ignored (Desai, Mallya, Chopra & Singh, 2005), (Padmanabhan, Governatori, Sadiq, Colomb & Rotolo, 2006). In particular (zur Muehlen, Indulska & Kamp, 2007) provide a valuable representational analysis to understand the synergies between process modeling and rule modeling.

It is obvious that the modelling of controls will be undertaken as rules, although the question of appropriate formalism is still under studied. A plethora of proposals exist both in the research community on formal mod-

elling of rules, as well as in the commercial arena through business rule management systems.

Historically, formal modelling 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, …) 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 starting point for logical investigation of the basic normative notions and it offers a very idealised 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 & Jones, 2002). Very often normative statements pertinent to business processes, and in particular contracts, specify conditions about when other conditions in the document have nor been fulfilled, that is when some (contractual) clauses have been violated. Hence any formal representation, to be conceptually faithful, has to been able to deal with this kind 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 modelling 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.

Below we present an account of the various proposals for formal modelling of controls. (Governatori, 2005),(Governatori & Milosevic, 2006) have proposed FCL (Formal Contract Language) as a candidate for control modelling, which has proved effective due to its ability to reason with violations. A rule in FCL is an expression of the form $r{:}A_1,...,A_n \Rightarrow B$, where r is the name of the rule (unique for each rule), $A_1,...,A_n$ are the premises, (propositions in the logic), and B is the conclusion of the rule (again B is a 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 ¬ *p*, is a proposition;
- if *p* is a proposition then *Op* is an obligation proposition and *Pp* is a permission proposition; obligation propositions and permission propositions are deontic propositions
- if $p_1,...,p_n$ are obligation propositions and *q* is a deontic proposition, then $p_1 \otimes ... \otimes p_n \otimes q$ 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 $O_s SendInvoice$ means that the supplier *s* has the obligation to send the invoice to the purchaser, and $P_p ChargePenalty$ means that the purchaser *p* is entitled (permitted) to charge a penalty to the supplier. A reparation chain, for example:

$$O_s ProvideGoodsTimely \otimes O_s OfferDiscout \otimes P_p ChargePenalty$$

captures obligations and normative positions arising in response to violations of obligation. Thus the expression above means that the supplier has the obligation to send the goods in a timely manner, but in case she does not comply with this (i.e., she violates the obligation do so) then she has the "secondary" obligation to offer a discount for the merchandise, and in case that she fails 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, while a normative rule allows us to conclude a normative position (i.e., an obligation, a permission or a prohibition, where a prohibition is $O\neg$ or equivalently $\neg P$). 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.

FCL offers two reasoning modules: (1) a normaliser 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 (Governatori, 2005).

There have been some other notable contributions from research on the matter of control modelling. (Goedertier & Vanthienen, 2006) presents a logical language PENELOPE, that provides the ability to verify temporal constraints arising from compliance requirements on effected business processes. (Kuster, Ryndina & Gall, 2007) provide a method to check compliance between object lifecycles that provide reference models for data artefacts e.g. insurance claims and business process models. (Giblin, Muller & Pfitzmann, 2006) who 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, Johnson, Kiernan & Leymann, 2006) has presented a workflow architecture for supporting Sarbanes-Oxley Internal Controls, which include 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, Sergot, Sallé & Bartolini, 2005) study the performance of business contract based on their formal representation. (Desai, Narendra& Singh, 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, Chesani, Gavanelli, Lamma, Mello & Torroni, 2006).

4.2 Process Model Enrichment

As discussed previously, modelling the controls is only the first step towards compliance by design. The second essential step is the enrichment of process models with compliance requirements (i.e. the modelled 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 been recently some efforts towards support for business process modelling against compliance requirements. In particular, the work of (zur Muehlen & Rosemann, 2005) and (Neiger, Churilov, zur Muehlen & Rosemann, 2006) provides 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, Governatori & Namiri, 2007) propose an approach based on control tags to visualize internal controls on process models.

(Liu, Muller & Xu, 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, business intelligence etc. Noteworthy in research literature with respect to compliance monitoring, is the synergy with process mining techniques (van der Aalst, van Dongen, Herbst, Maruster, Schimm & Weijters, 2003), (van Dongen, de Medeiros, Verbeek, Weijters & van der Aalst, 2005) which provide the capability to discover runtime 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 & Reporting, Microsoft Office Solutions Accelerator for Sarbanes-Oxley, SAP GRC (Governance, Risk and Compliance) Solution, as well as niche vendors such as OpenPages, Paisley Consulting, Qumas Inc and several others (Caldwell & Eid, 2008).

Software solutions and tools for compliance are typically found under the umbrella of another technology such as business intelligence or business rules management etc. As such compliance vendors are not easily identified directly. Further, whereas 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, e.g. a Business Controls & Reporting tool designed to help users manage processes, controls, and information subject to Sarbanes Oxley 404.

5 Discussion and Outlook

As the importance of governance, risk and compliance 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), i.e. achieving a balance between control and business objectives.

This has been a driver of the research presented in this chapter. The methodology presented in section 3 provides a systematic means of aligning business and control objectives. However, several open issues still remain.

A number of proposals exist for *modelling controls* (see section 4.1). Although several proposals provide a powerful and conceptually faithful means of capturing controls, it still remains to be studied, how these formal models can be deployed in practice.

Effective framework for modelling controls is a necessary prerequisite to studying the alignment between business and control objectives. We have demonstrated how such models can provide a means of enriching and subsequently analysing business process models, which in turn can be used for *model driven compliance enforcement*.

Enriched business process models bring the added benefit of providing the *capability for diagnostics* (see section 3.4). That is provide a means of understanding what needs to be done in order to achieve (an acceptable degree of) compliance (Lu, Sadiq & Governatori, 2007). This is a hard problem in general due to the semantically rich nature of the involved models.

A theoretically rigorous and practically feasible means of control modelling supported by a powerful analysis machinery that provides diagnostic support for comparing business and control objectives has the potential to create a holistic approach to compliance management, by not only providing preventative and detective techniques, but also corrective recommendations.

Future research endeavors in this area should strive towards 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.

References

van der Aalst, W.M.P., van Dongen, B.F., Herbst, J., Maruster, L., Schimm, G., & Weijters, A.J.M.M. (2003). Workflow Mining: A Survey of Issues and Approaches. Data & Knowledge Engineering, 47, 237 – 267.

van der Aalst, W.M.P., Alves de Medeiros, A.K., & Weijters, A.J.M.M. (2006). Process Equivalence: Comparing Two Process Models Based on Observed Behavior. In Proceedings of the 4th International Conference on Business Process Management, pp. 129-144, Vienna, Austria 2007. Springer-Verlag.

ASX (2006) Australian Securities Exchange Principles of Good Governance, Recommendation 7.1, Nov. 2006. www.asx.gov.au (last accesses June 01, 2008)

Agrawal, R., Johnson, C., Kiernan, J., & Leymann, F. (2006). Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. In Proceedings of the 22nd International Conference on data Engineering,2006, Atlanta, GA, USA. IEEE Computer Society.

AUSTRAC (2006) Australian Transaction Reports and Analysis Centre Supervisory Framework. www.austrac.gov.au/files/supervisory_framework.pdf (last accessed June 01, 2008)

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

BPM Forum (2006). CEE: The Future. Building the Compliance Enabled Enterprise. Report producedby Global Fluency in partnership with: AXS-One, Chief Executive Magazine and IT Compliance Institute.

Caldwell, F. & Eid, T. (2007) Magic Quadrant for Finance Governance, Risk and Compliance Management Software, 2007. Gartner RAS Core Research Note G00145150, 1 Feb 2007, RS196 0906 2007.

Caldwell, F., & Eid, T. (2008) Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms. ID. G00158295. June 2008. Gartner Research .

Carmo, J., &Jones, A.J.. (2002). Deontic logic and contray-to-duties. In Handbook of Philosophical Logic, 2nd Edition, pages 265–344. Springer, 2002.

COSO –TheCommittee of Sponsoring Organizations of theTreadway Commission. (1994) InternalControl – Integrated Framework. May 1994.

Desai, N., Nanjangud, N.C., & Singh, M.P. (2008) Checking Correctness of Business Contracts via Commitments. Proc. Of 7th Int. Conf. on Autonomous Agents

and Multiagent Systems (AAMAS2008), Padgham, Parkes, Müller and Parsons (eds.), May, 12-16, 2008, Estoril, Portugal

Desai, N., Mallya, A.U., Chopra, A.K., & Singh, M.P. (2005). Interaction Protocols as Design Abstractions for Business Processes. IEEE Transaction on Software Engineering 31(12) 1015-1027.

van Dongen, B.F., de Medeiros, A.K.A., Verbeek, H.M.W., Weijters, A.J.M.M., & van der Aalst, W.M.P. (2005). The ProM Framework: A New Era in Process Mining Tool Support. In Proceedings of 26th International Conference Applications and Theory of Petri Nets, pp 444-454, Miami, USA, 2005. Springer-Verlag.

Farrell, A. D. H., Sergot, M.J., Sallé, M., & Bartolini, C. (2005). Usingthe Event Calculus for Tracking the Normative State in Contracts. International Journal of Cooperative Information Systems 14 (2-3): 99-129.

Giblin, C., Muller, S., & Pfitzmann, B. (2006). From Regulatory Policies to EventMonitoring Rules: Towards Model Driven Compliance Automation. IBM Research Report. Zurich Research Laboratory. Oct. 2006.

Goedertier, S., & Vanthienen, J. (2006). Designing Compliant Business Processes with Obligations and Permissions. In Eder, J., & Dustdar, S. et al. (Eds.) Proceedings of Workshop on Business Process Design, pp. 5-14, Vienna, Austria 2006. LNCS 4103 Springer-Verlag.

Governatori, G., Hoffmann, J., Sadiq, S., & Weber, I. (2008) Detecting Regulatory Compliance for Business Process Models through Semantic Annotations. 4th International Workshop on Business Process Design (BPD'08). In conjunction with the 6th International Conference on Business Process Management, Milan, Italy. 1-4 September 2008.

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

Governatori, G., & Milosevic, Z. (2006) A Formal Analysis of a Business ContractLanguage. International Journal of Cooperative Information Systems 15(4), 659-685.

Governatori, G., Milosevic, Z, & Sadiq, S. (2006). Compliance Checking betweenBusiness Processes and Business Contracts. In Proceedings of the 10th IEEE Conference on Enterprise Distributed Object Computing, Hong Kong.

Governatori, G., & Rotolo, A. (2006) Logic of Violations: A Gentzen System for Reasoning on Contrary-To-DutyObligations. Australasian Journal of Logic, 4, 193–215.

Governatori, G., Rotolo, A., & Sartor. G. (2005) Temporalised normative positions in defeasible logic. In A. Gardner, editor, Procedings of the 10th International Conference on Artificial Intelligence and Law, pages 25-34. ACM Press, 2005.

Hagerty, J., Hackbush, J., Gaughan, D., & Jacobson, S. (2008) The Governance, Risk Management, and Compliance Spending Report, 2008–2009: Inside the $32B GRC Market. March 25, 2008. AMR Research, Boston USA.

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

Kuster, J., Ryndina, K., & Gall, H., (2007). Generation of Business Process Models for Object Life Cycle. In Proceedings of the 5th International Conference on Business Process Management, pp. 165-180, Brisbane, Australia. Springer-Verlag.

Liu, Y., Muller, S., & Xu, K. (2007) A Static Compliance Checking Framework for Business Process Models. IBM Syst. J. 46 (2007) 335–361

Lu, R., Sadiq, S., & Governatori, G. (2008) Compliance Aware Business Process Design. 3rd International Workshop on Business Process Design (BPD'07). In conjunction with the 5th International Conference on Business Process Management, 24-28 September 2007. Springer Berlin / Heidelberg LNCS Volume 4928/2008, Pg. 120-131.

Neiger, D., Churilov, L., zur Muehlen, M., & Rosemann, M. (2006) Integrating Risks in Business Process Models with Value Focused Process Engineering. In: Proceedings of the 2006 European Conference on Information Systems (ECIS 2006), Goteborg, Sweden, June 12-14, 2006.

Padmanabhan, V., Governatori, G., Sadiq, S., Colomb, R., & Rotolo, A. (2006). Process Modeling: The Deontic Way. In M. Stumptner, S. Hartmann and Y. Kiyoki, editors, Australia-Pacific Conference on Conceptual Modeling, pp. 75-84, CRPIT 53.

Pesic, M., & van der Aalst, W.M.P. (2006) A Declarative Approach for Flexible Business Processes. In J. Eder and S. Dustdar, editors, Business Process Management Workshops, Workshop on Dynamic Process Management (DPM 2006), volume 4103 of Lecture Notes in Computer Science, pages 169-180. Springer-Verlag, Berlin, 2006.

Sadiq, S., Sadiq, W., & Orlowska, M. (2005) A Framework for Constraint Specification and Validation in Flexible Workflows. Information Systems, 30, 5: 349-378

Sadiq, S., Governatori, G., & Naimiri, K. (2007) Modeling Control Objectives for Business Process Compliance. In Proceedings of the 5th International Conference

on Business Process Management, pp. 149–164, Brisbane, Australia 2007. Springer-Verlag.

Sartor, G. (2005). Legal Reasoning: A Cognitive Approach to the Law. Springer,

Zur Muehlen, M., Indulska, M., & Kamp, G. (2007) Business Porcess and businessRule Modelling Languages for Compliance Management: A Representaitonal Analysis. 26th International Conference on Conceptual Modelling – ER2007 – Tutorials, Posters, Panels and Industrial Contributions, Auckland, New Zealand. Nov 2007.

zur Muehlen, M., & Rosemann, M. (2005). Integrating Risks in Business Process Models. In Proceedings of 16th Australasian Conference on Information Systems. Sydney, Australia.