Managing Regulatory Compliance in Business Processes

Shazia Sadiq and Guido Governatori

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),

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

J. vom Brocke and M. Rosemann (eds.), *Handbook on Business Process Management 2,*
International Handbooks on Information Systems,
DOI 10.1007/978-3-642-01982-1_8, © Springer-Verlag Berlin Heidelberg 2010

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 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 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 approach 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 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

[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).

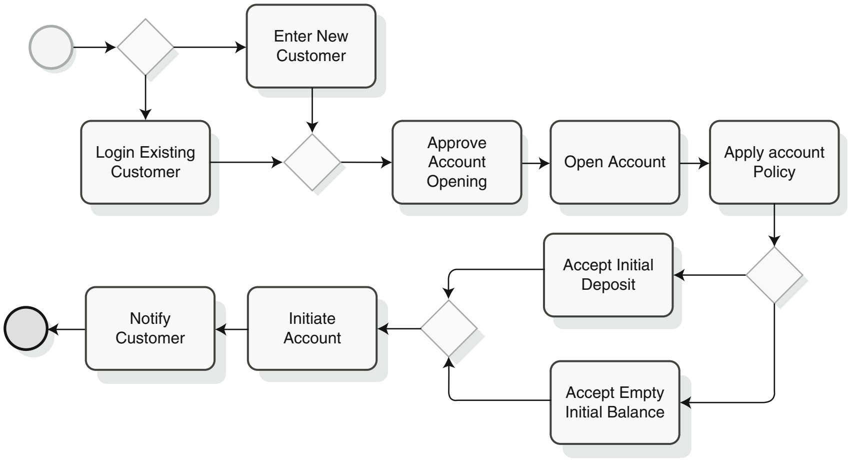

Fig. 1 Example account-opening process

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

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.

[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).

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.

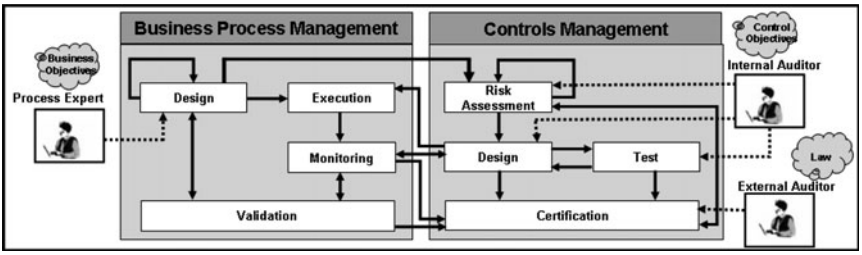

Fig. 2 Interconnect of process management and controls management

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:

<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 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

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.

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 not the focus of this paper but nonetheless 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, thereby providing the ability to discover hidden dependencies, and view in holistic context, while maintaining a comprehensible

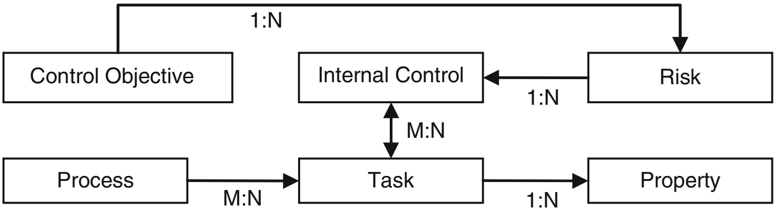

Fig. 3 Relationships between process modeling and control modeling concepts

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 et al. 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 Fig. 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

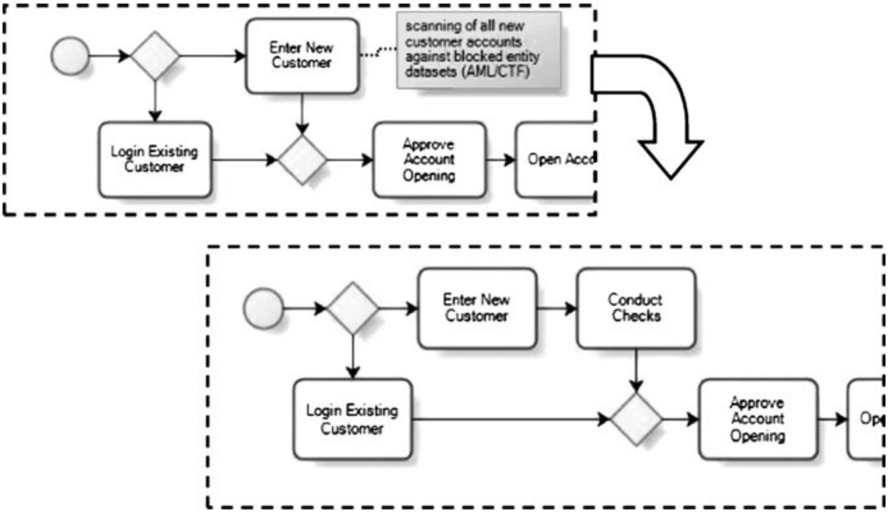

Fig. 4 Process annotation and resultant redesign

the process model presented in Fig. 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 analyze the model for measures such as *compliance degree* (Lu et al. 2008), 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 et al. 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.

The methodology as presented so far can be summarized as in Fig. 5. Note however, that the Sects 3.1–3.4 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-*

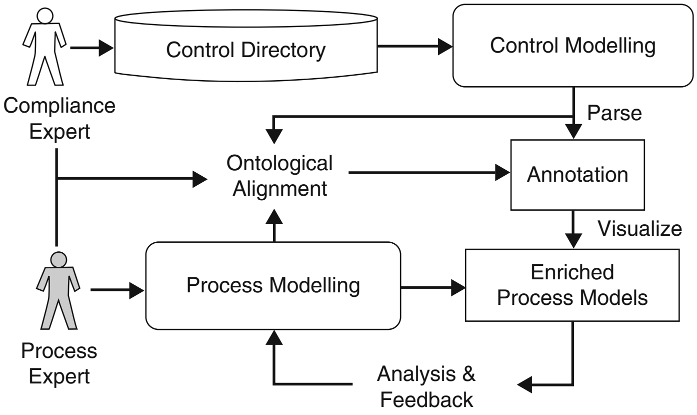

Fig. 5 Summary of design time support in the methodology

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) 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 that holds challenges for various communities including information systems; business software development; legal, cultural, and 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 Sects 3.3–3.4.

4.1 Modeling 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 et al. 2005; Padmanabhan et al. 2006). In particular, zur Mühlen et al. (2007) provide a valuable representational analysis to understand the synergies between process modeling and rule modeling.

It is obvious that the modeling of controls will be undertaken as rules, although the question of appropriate formalism is still understudied. 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 of controls. Governatori (2005) and Governatori and Milosevic (2006) have proposed FCL (formal contract language) as a candidate for control modeling, which has proved effective due to its ability to reason with violations. A rule in FCL is an expression of the form r: $A_1,\ldots, A_n \Rightarrow B$, where r is the name of the rule (unique for each rule), $A_1,\ldots, A_n$ 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 $\neg p$ 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 $p_1,\ldots,p_n$ are obligation propositions and q is a deontic proposition, then $p_1 \otimes \ldots \otimes p_n \otimes q$ 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. A reparation chain, for example:

$$O_s\ \mathit{Provide\ Goods\ Timely} \otimes O_s\ \mathit{Offer\ Discout} \otimes P_p\ \mathit{Charge\ Penalty}$$

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, 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 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 (Governatori 2005).

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. Kuster 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) has 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 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 Sect. 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–Oxley 404.

5 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.

A number of proposals exist for *modeling controls* (see Sect. 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 modeling 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 analyzing 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 Sect. 3.4): that is, provide a means of understanding as to what needs to be done in order to achieve (an acceptable degree of) compliance (Lu et al. 2008). 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 modeling 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 providing not only preventative and detective techniques but also corrective recommendations.

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.

References

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

Alberti M, Chesani F, Gavanelli M, Lamma E, Mello P, Torroni P (2006) Compliance verification of agent interaction: a logic based tool. Appl Artif Int 20(2–4):133–157

ASX (2006) Australian securities exchange principles of good governance, recommendation 7.1, Nov. 2006. www.asx.gov.au (last accesses June 01, 2008)

AUSTRAC (2006) Australian transaction reports and analysis centre supervisory framework. www.austrac.gov.au/files/supervisory_framework.pdf. Accessed 01 Jun 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, 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 AJ (2002) Deontic logic and contrary to duties. In: Gabbay D, Guenther F (eds.) Handbook of Philosophical Logic, 2nd edn., vol. 8, pp 265–343

COSO –The committee of sponsoring organizations of the treadway commission (1994) Internal control – integrated framework. May 1994

Desai N, Mallya AU, Chopra AK, Singh MP (2005) Interaction protocols as design abstractions for business processes. IEEE Trans Softw Eng 31(12):1015–1027

Desai N, Nanjangud NC, Singh MP (2008) Checking correctness of business contracts via commitments. In: Padgham L, Parkes DC, Müller J, Parsons S (eds) Proceedings of 7th International conference on autonomous agents and multiagent systems (AAMAS2008), Estoril, Portugal, 12–16 May 2008

Farrell ADH, Sergot MJ, Sallé M, Bartolini C (2005) Using the event-calculus for tracking the normative state in contracts. Int J Coop Infor Syst 14(2–3):99–129

Giblin C, Muller S, Pfitzmann B (2006) From regulatory policies to event monitoring rules: towards model driven compliance automation. IBM Research Report. Zurich Research Laboratory

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, Springer, Vienna, Austria, pp 5–14, LNCS 4103

Governatori G (2005) Representing business contracts in RuleML. Int J Coop Infor Syst 14 (2–3):181–216

Governatori G, Milosevic Z (2006) A formal analysis of a business contract language. Int J Coop Infor Syst 15(4):659–685

Governatori G, Rotolo A (2006) Logic of violations: a gentzen system for reasoning on contrary-to-duty obligations. Austral J Logic 4:193–215

Governatori G, Rotolo A, Sartor G (2005) Temporalised normative positions in defeasible logic. In: Gardner A (ed) Proceedings of the 10th International conference on artificial intelligence and law, ACM Press, pp 25–34

Governatori G, Milosevic Z, Sadiq S (2006) Compliance checking between business processes and business contracts. In: Proceedings of the 10th IEEE conference on enterprise distributed object computing, Hong Kong

Governatori G, Hoffmann J, Sadiq S, Weber, I (2008) Detecting regulatory compliance for business process models through semantic annotations. In: 4th International workshop on business process design (BPD'08). In conjunction with the 6th International Conference on Business Process Management, Milan, Italy. pp 1-4

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

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. Springer, Brisbane, Australia, pp 165–180

KPMG Advisory (2005) The compliance journey: balancing risk and controls with business improvement

Liu Y, Muller S, Xu K (2007) A static compliance checking framework for business process models. IBM Syst J 46:335–361

Lu R, Sadiq S, Governatori G (2008) Compliance aware business process design. Third 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, LNCS Volume 4928/2008, pp 120–131

Neiger D, Churilov L, zur Mühlen 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, 12–14 June 2006

Padmanabhan V, Governatori G, Sadiq S, Colomb R, Rotolo A (2006) Process modeling: the deontic way. In Stumptner M, Hartmann S, Kiyoki Y (eds) Australia–Pacific conference on conceptual modeling, pp 75–84, CRPIT 53

Pesic M, van der Aalst WMP (2006) A declarative approach for flexible business processes. In: Eder J, Dustdar S (eds) Business process management workshops, workshop on dynamic process management (DPM 2006), volume 4103 of Lecture notes in computer science. Springer-Verlag, Berlin, pp 169–180

Sadiq S, Sadiq W, Orlowska M (2005) A framework for constraint specification and validation in flexible workflows. Inf Syst 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, Springer, Brisbane, Australia, pp 149–164

Sartor G (2005) Legal reasoning: a cognitive approach to the law. Springer, Berlin

van der Aalst WMP, van Dongen BF, Herbst J, Maruster L, Schimm G, Weijters AJMM (2003) Workflow mining: a survey of issues and approaches. Data Knowl Eng 47:237–267

van der Aalst WMP, Alves de Medeiros AK, Weijters AJMM (2006) Process equivalence: comparing two process models based on observed behavior. In: Proceedings of the 4th

International conference on business process management, Vienna, Austria, 2007. Springer, pp 129–144

van Dongen BF, de Medeiros AKA, Verbeek HMW, Weijters AJMM, van der Aalst WMP (2005) The ProM Framework: a new era in process mining tool support. In: Proceedings of 26th International conference applications and theory of petri nets, Springer, Miami, USA, pp 444–454

zur Mühlen M, Rosemann M (2005) Integrating risks in business process models. In: Proceedings of 16th Australasian conference on information systems. Sydney, Australia

zur Mühlen M, Indulska M, Kamp G (2007) Business process and business rule modelling languages for compliance management: a representational analysis. In: 26th International Conference on Conceptual Modelling – ER2007 –Tutorials, Posters, Panels and Industrial Contributions, Auckland, New Zealand