Exploring Features of a Full-Coverage Integrated Solution for Business Process Compliance*

Cristina Cabanillas, Manuel Resinas, and Antonio Ruiz-Cortés

Universidad de Sevilla, Spain
{cristinacabanillas,resinas,aruiz}@us.es

Abstract. The last few years have seen the introduction of several techniques for automatically tackling some aspects of compliance checking between business processes and business rules. Some of them are quite robust and mature and are provided with software support that partially or fully implement them. However, as far as we know there is not yet a tool that provides for the complete management of business process compliance in the whole lifecycle of business processes. The goal of this paper is to move towards an integrated *business process compliance management system (BPCMS)* on the basis of current literature and existing support. For this purpose, we present a description of some compliance-related features such a system should have in order to provide full coverage of the business process lifecycle, from compliance aware business process design to the audit process. Hints about what existing approaches can fit in each feature and challenges for future work are also provided.

Keywords: business process compliance, feature analysis, compliance management system, integration framework, business process lifecycle.

1 Introduction

Much work has been published on business process compliance in the last decade. Many organizations are concerned with ensuring compliance between business processes and regulations, and this has awoken the interest of many researchers. There are some well-defined and automatically supported approaches for Post-Design Time Compliance Checking (PDTCC) [1, 2], for Run-Time Compliance Checking (RTCC) [3], and for Backward Compliance Checking (BCC) [4, 5]. However, most of these approaches focus both on a specific kind of compliance rules (e.g. those concerning only control flow) and on a concrete checking moment (being it before, during or after the execution of a business process).

So, compliance checking techniques have been developed but, to the best of our knowledge, a compliance management system that gives support to the

* This work has been partially supported by the European Commission (FEDER), Spanish Government under the CICYT project SETI (TIN2009-07366); and projects THEOS (TIC-5906) and ISABEL (P07-TIC-2533) funded by the Andalusian Local Government.

C. Salinesi and O. Pastor (Eds.): CAiSE 2011 Workshops, LNBIP 83, pp. 218–227, 2011.

whole lifecycle of business processes is still missing. Coming up with a system that puts them all together would be very useful for several reasons: (i) some of the developed techniques for compliance checking are complementary, i.e. some approaches complement the results of other approaches; (ii) applying compliance mechanisms addressing only a part of the aspects of a business process and/or in a single period of time (i.e. design time or run time) does not guarantee that the business processes of an organization are compliant with all the rules they have to fulfill; and (iii) a system that controls all kinds of business process compliance would help organizations to be prepared for audits, and would make auditors' work easier.

With this paper we pretend to walk a step forward in this direction by presenting a description of some compliance-related features a *business process compliance management system (BPCMS)* should have in order to provide full coverage of the business process lifecycle, from compliance aware business process design to post-execution evaluation, including audit process as well. Besides specifying the desired features of a BPCMS, hints about what existing approaches for business process compliance checking can fit in each feature and challenges for future work are also provided. We build on the existing literature about business process compliance to carry out this work.

The paper is structured as follows: Section 2 presents a view of a compliance-aware business process lifecycle; in Section 3 we explain some features required to provide full-coverage of the lifecycle, jointly with an outline of the main literature analysed to perform this work; Section 4 contains some conclusions and several challenges that must be faced to develop a full-coverage integrated BPCMS.

2 Compliance-Aware Business Process Lifecycle

We have extended the business process lifecycle described by Weske [6] to make it compliance-aware, i.e., to include aspects related to business process compliance. We rely on the descriptions provided by Weske to briefly define each phase of the business process lifecyle and foresee the aspects it would require to be compliance-aware. There are so-called compliance lifecycles in literature, such as the one in [3, 7]. This lifecycle differs from our proposal in that it is directly focused on compliance, while we focus on business process management.

In the *design phase* business processes are identified, reviewed, validated, and represented by business process models using a particular notation. Collaborative capabilities for the jointly modelling of the processes and design assistance would be helpful to design compliant business processes.

In the *analysis phase* business process models are analysed by means of validation, simulation and/or verification techniques, and improved so that they actually represent the desired business processes and that they do not contain any undesired properties. Regarding compliance, capabilities to carry out compliance checkings, to have corrective advising and to perform simulation of compliance issues are required.

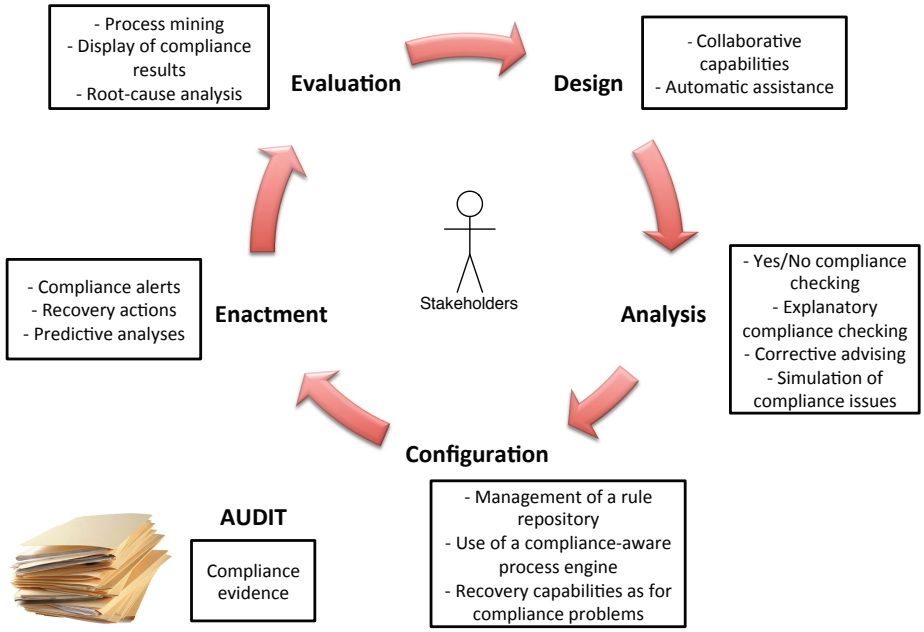

Fig. 1. Compliance-aware business process lifecycle

Once the business process models are designed and verified, the business processes need to be implemented. An implementation platform is chosen during the *configuration phase*, and it is configured together with the employees system interactions and the integration of software systems existing in the organization and the business process management system. Mechanisms to manage rule repositories and a compliance-aware process engine have to be considered during the configuration phase. Then, the implementation of the business processes needs to be tested, so integration and performance tests are carried out.

The process *enactment phase* encompasses the actual run time of the business process, in which process monitoring plays an important role for providing accurate information on the status of business process instances. Once again, mechanisms to check business process compliance at run time, to alert about found problems, to recover from violations and to predict possible future problems are required.

Finally, the *evaluation phase* uses information available to evaluate and improve business process models and their implementations. Execution logs are evaluated using business activity monitoring (BAM) and process mining techniques. These techniques have to be extended to include compliance aspects, root-cause analyses should be carried out, and the ability of displaying the results of compliance analyses should be considered.

Figure 1 shows what we are calling *compliance-aware business process lifecycle*. As depicted, the five phases of the business process lifecycle described in [6] are

surrounded by compliance-related features. These are some *specific* features a BPCMS should provide in each phase to include compliance issues in business process management. They will be explained in detail in Section 3. We have included *audit* as an element external to the lifecycle because it makes sense in compliance domain but it does not in generic business process management. Proofs that provide compliance evidence are necessary to perform audits.

3 Features for Compliance Support

This section contains a description of the features required in every phase of the compliance-aware business process lifecycle introduced above. These are the desired features of a full-coverage BPCMS.

3.1 Design

Creating business processes aware of compliance is the first step towards ensuring that processes fulfill the business rules imposed to an organization by regulations and legislations, by normative rules that help guarantee business quality such as ISO/IEC 20000, and by the organization itself. Two groups of features have been identified:

- **Collaborative capabilities.** Joining processes and rules is a complex task, which demands great expertise about the specific business processes carried out in an organization, the rules that must be fulfilled and their application to these business processes. Not making a clear separation between *what business processes must do* and *the features introduced because of the inclusion of rules* may affect the resulting business process models negatively. It means that when modelling business processes aware of compliance issues, the modeller must not disregard the final goal of the process and the services it has to provide to the organization in order to avoid changing its behaviour because of the rules. To prevent this problem, a *business expert* and a *compliance expert* should put their effort on respectively identifying and modelling business processes, and interpreting and modelling business rules, and then put together the individual work with the aim of providing a single *compliance-aware business process model*. Specific definitions for these two roles can be found in [8]. Offering collaborative design support (i.e. collaborative business process modelling) and social capabilities such as those characteristic of wikis and social networks (e.g. addition of comments and forums) would be desirable.
- **Automatic assistance.** An alternative that does not require the existence of separate roles consists of providing the tool with a suggestion mechanism that automatically assists the modeller during the design of the process to make it comply with the business rules. For this to be possible the rules must have been previously defined, which in turn requires minimally knowing the activities the business process is made up of beforehand. To the best of our knowledge, there is not yet a tool that provides this design assistance to the user with the aim of modelling compliant business processes.

3.2 Analysis

Performing compliance checking after the design of a business process is necessary to avoid behavioural problems at run time, as well as to ensure that all the proofs necessary to successfully pass subsequent compliance audits will be created during execution. Seeking compliance problems requires examining the behaviour of the process regarding semantics, that is, analysing the process from execution perspective to find out unexpected behaviours, e.g. mandatory activities that may not be executed due to XOR splits. This matter, together with the fact that full compliance checking must consider rules involving the four following aspects of business process: control flow, data, time and resources, makes the full analysis of compliance-aware business process models quite difficult. This is the main reason why most of the existing approaches for compliance checking deal only with control flow issues [1, 2, 4, 9, 10, 11, 12]. However, addressing data aspects is increasingly awaking the interest of researchers [13]. For instance, Cabanillas et al. have developed a procedure aimed at making data-related compliance checking easier by automatically generating a data-centered view of business processes [14]. This view can be used as input of algorithms to check for data-related compliance problems such as those described in [15]. Taking all this into account, a full-coverage BPCMS should contain the next features:

- **Yes/No compliance checking.** Sometimes the analyst requires quickly finding out whether a business process model is compliant with rules without going into detail. Therefore, this requirement should be available both to check for a single rule and to check for the whole set of rules that have to be applied to the business process. Some approaches supporting Yes/No response are described in [1, 9, 10].
- **Explanatory compliance checking.** Giving an explanation of an identified problem is very useful to the analyst and/or modeller of the business process. Most of the existing approaches, out of those that include this feature, expose the explanations in the form of *counterexamples*, i.e., a demonstration or example of how a rule can be violated. This output must be as real as possible, meaning that the counterexample must be traced back to the business process model in order to comprehend what it actually means, no matters what the formalism to detect the compliance problem was. For example, OPAL [2] applies model-checking algorithms to check business process compliance and, in case of violations, it returns counterexamples to demonstrate the existence of such problems. Root-cause analyses can be used to explain compliance violations as well [16].
- **Corrective advising.** Having at disposal an assistant that guides the user towards solving the compliance problems detected would be useful (and helpful) to complement the two previous features. Ideally, more than one corrective action may be suggested to the user, who can choose how to repair violations. In [17], Ghose et al. present an approach to detect and repair non-compliant business processes.

– **Simulation of compliance issues.** Including a simulator of business process execution that takes compliance issues into account can help detect unexpected behaviour by simulating the execution of the business processes (step by step) with value configurations obtained from the analysis of previous executions or from the specific domain knowledge of the analyst.

3.3 Configuration

Before executing a business process its instrumentation is required, i.e., it is important to configure the BPCMS as for the following features:

– **Management of a rule repository.** Although it has already been glimpsed in the features of the previous two phases, having a repository of rules and enabling the system to access it is of utmost importance. In this phase, mechanisms to select the business rules that have to be checked at run time and to configure other parameters referring to the compliance rules that have to applied are required.
– **Use of a compliance-aware process engine.** As we need to keep a trace of business process execution for post-execution checks, it is necessary to set at which moments of a business process execution the events to be stored will be triggered (compliance evidence included), how they will be captured and processed by the process engine, and the way they will be stored.
– **Recovery capabilities as for compliance problems.** The BPCMS must allow selecting the recovery actions that can be applied at run time for a specific business process in case of compliance violation, from all the possible recovery actions.

3.4 Enactment

RTCC has barely been addressed in compliance-related work. The work in [3] and [18] are two of the few approaches we have found regarding compliance checking at run time. However, no mention to the features desired for this phase of business process lifecycle is included in them. During the execution of a business process the BPCMS must ensure the appropriate rules are being fulfilled and the compliance evidence necessary for subsequent audits is being created. Furthermore, the next features must be part of the BPCMS:

– **Compliance alerts.** The tool must be enabled to show alerts about compliance problems arised at run time, as well as to automatically send notifications about them to the person in charge.
– **Recovery actions.** Besides the appropriate alerts, the execution of a business process can either continue after a compliance violation, either ignoring the problem or after the necessary recovery action(s), or get blocked until being manually revised and/or repaired. Namiri et al. present some recovery actions to be considered (including some of the aforementioned) [8].

– **Predictive analyses.** The system must be able to be ahead of future problems that may occur during the execution of a process instance, thus preventing their appearance by means of proper alerts that cause human reactions or by automatically performing recovery actions. This predictive analyses can be carried out from history logs containing previous instance executions.

3.5 Evaluation

Several techniques can be carried out to assess the degree of compliance of a business process execution:

– **Process mining.** After the execution of a process instance all the information generated must be in an event log. Logs will contain all the information necessary to cover the four aspects of the business processes mentioned before in this paper. Van der Aalst et al. have defined a business process compliance checker that performs BCC from logs by means of process mining [5]. It is implemented in tool LTL Checker, a plugin of ProM[1]. However, temporal constraints seem to be unconsidered in this approach. Another BCC approach is explained in [4], where Rozinat et al. introduce tool Conformance Checker (also included in ProM), which compares an a-priori business process model with the observed reality stored in some MXML log. This technique addresses only control flow.
– **Display of compliance results.** Once compliance has been checked, a mechanism to show the results is necessary. The use of a *Compliance Governance Dashboard (CGD)* that lets the user choose among several levels of abstraction, so all the information required to perform both internal and external audits can be drilled down, would be very useful [7].
– **Root-cause analysis.** From event logs and CGDs, root-cause analyses can be performed. These analyses study the behaviour of instances of a business process to find out the cause of compliance violations, i.e., give explanations. Rodriguez et al. carry out root-cause analyses based on decision trees from CGDs in [20], with the support of the EU research projects COMPAS and MASTER. From the analysis results, the system should also offer suggestions about corrective actions that help avoid compliance problems in future executions of a business process.

3.6 Audit

The system must be prepared to allow the execution of internal audits aimed at performing routine controls by the organization, and external audits carried out by compliance experts unconnected with the organization and responsible for checking whether this complies with the rules. Proofs for compliance can be given in the form of documents that corroborate the business process is being executed in accordance with the corresponding compliance rules. As stated in [21], "documentation is a key element of each audit. Important objectives of documentation include providing evidence [...] This results in a number of different tasks, including

[1] ProM is an extensible framework for process mining [19].

Table 1. Existing feature coverage of the desirable features of a full-coverage BPCMS

Compliance-aware BP lifecycle phase	Feature	Coverage	Implementation
Design	Collaborative capabilities		
	Automatic assistance		
Analysis	Yes/No compliance checking	[1] [9] [10] [11] [12] [15]	[1] [9] [10] [11] [12] [15]
	Explanatory compliance checking	[2] [16]	[2] [16]
	Corrective advising	[16] [17]	[16] [17]
	Simulation of compliance issues		
Configuration	Management of a rule repository		
	Use of a compliance-aware process engine	[3]	[3]
	Recovery capabilities as for compliance problems		
Enactment	Compliance alerts	[8]	
	Recovery actions	[8]	
	Predictive analyses		
Evaluation	Process mining	[4] [5]	[4] [5]
	Display of compliance results	[7]	[7]
	Root-cause analysis	[20]	[20]
Audit	Compliance evidence		

ensuring the completeness of the information, the traceability of the findings and recommendations, and providing a safeguard function. [...] The concept of audit is inseparable from documentation". This need of evidence is also remarked in normative rules such as ISO/IEC 20000, which calls for the storage of reports to prove compliance. The structure and storage of proofs must be perfectly defined.

4 Conclusions and Open Challenges

Although guaranteeing business process compliance may be impossible, if an organization limits the scope of compliance checking to one of the phases of business process lifecycle, ensuring that their business processes comply with all the rules the organization is subjected to becomes even harder. In this paper we have walked a step towards the definition of a BPCMS that covers the whole business process lifecycle by defining some compliance-related features the system should contain in every phase to ease the fulfillment of rules. The features have been gathered from existing literature.

Table 1 collects the aforementioned features, together with existing approaches that could be used to cover them. Blank cells represent features never addressed before. As shown in the table, there are not yet approaches to deal with compliance-aware business process design as understood in this paper. Approaches facing analysis phase focus on compliance checking and do not consider simulation functionalities. Specific work on configuration of a BPCMS should be done. As far as enactment phase is concerned, some approaches mention the use of alerts and recovery actions, but there is not yet a full implementation of these features. Predictive analysis is still to be done. However, features mentioned for

evaluation are widely covered by current approaches. The collection of compliance evidence during business process execution is also disregarded in existing business process compliance related literature.

It is important to notice that in this paper we refer only to compliance-related features. Tool-related features such as scalability, efficiency and performance are out of its scope. Also the identification of candidate languages for modelling and executing processes, and the description of specific methods for compliance checking are beyond.

From this study we can conclude that many features are required for a BPCMS to cover the whole business process lifecycle, and only some of them have been partially described and/or implemented so far in literature. This reiterates the need of an integration framework that provides a full view of business process compliance management, both covering all the lifecycle phases and taking into account all the elements involved in business processes. Great efforts should be done to integrate all the existing solutions in such a framework.

In our opinion, the main challenges towards the design and development of a full-coverage integrated BPCMS are the following:

- We believe it would be interesting to provide solutions for all the blank cells present in Table 1, since having all the features described in Section 3 would be helpful to manage business process compliance. The empirical study carried out in [22] can complement the study we have performed giving an organization-centered perspective, thus showing the most critical features.
- Design an integration framework prepared to provide for compliance management in the whole business process lifecycle. For this purpose, assessing whether existing support tools can be integrated is necessary.
- Define a minimum catalogue of compliance rules the initial version of the system must cover and a language expressive enough to allow specifying the set of rules contained if the catalogue.
- Design an accessible, usable and friendly user interface (UI) for the system.
- Integrate the system with existing systems. In real scenarios instrumenting the process engine is not enough. Besides, events and proofs are spread over the different applications of the organization, so their integration with the BPCMS is required.

References

1. Awad, A., Decker, G., Weske, M.: Efficient compliance checking using bpmn-q and temporal logic. In: Dumas, M., Reichert, M., Shan, M.-C. (eds.) BPM 2008. LNCS, vol. 5240, pp. 326–341. Springer, Heidelberg (2008)
2. Liu, Y., Müller, S., Xu, K.: A static compliance-checking framework for business process models. IBM Systems Journal 46(2), 335–362 (2007)
3. Birukou, A., D'Andrea, V., Leymann, F., Serafinski, J., Silveira, P., Strauch, S., Tluczek, M.: An integrated solution for runtime compliance governance in SOA. In: Maglio, P.P., Weske, M., Yang, J., Fantinato, M. (eds.) ICSOC 2010. LNCS, vol. 6470, pp. 122–136. Springer, Heidelberg (2010)

4. Rozinat, A., van der Aalst, W.M.P.: Conformance checking of processes based on monitoring real behavior. Information Systems 33(1), 64–95 (2008)
5. van der Aalst, W.M.P., de Beer, H.T., van Dongen, B.F.: Process mining and verification of properties: An approach based on temporal logic. In: Chung, S. (ed.) OTM 2005. LNCS, vol. 3760, pp. 130–147. Springer, Heidelberg (2005)
6. Weske, M.: Business Process Management: Concepts, Languages, Architectures. Springer, Heidelberg (2007)
7. Silveira, P., Rodriguez, C., Casati, F., Daniel, F., D'Andrea, V., Worledge, C., Taheri, Z.: On the design of compliance governance dashboards for effective compliance and audit management. In: Workshop on Non-Functional Properties and SLA Management in Service-Oriented Computing (NFPSLAM-SOC) (2009)
8. Namiri, K., Stojanovic, N.: Using control patterns in business processes compliance. In: Weske, M., Hacid, M.-S., Godart, C. (eds.) WISE Workshops 2007. LNCS, vol. 4832, pp. 178–190. Springer, Heidelberg (2007)
9. Förster, A., Engels, G., Schattkowsky, T., Straeten, R.V.D.: Verification of business process quality constraints based on visual process patterns. In: TASE, pp. 197–208 (2007)
10. Governatori, G., Milosevic, Z., Sadiq, S.W.: Compliance checking between business processes and business contracts. In: EDOC, pp. 221–232 (2006)
11. Lu, R., Sadiq, S., Governatori, G.: Compliance aware business process design. In: Workshop on Business Process Design, BPD (2007)
12. Weber, I., Governatori, G., Hoffmann, J.: Approximate compliance checking for annotated process models. In: Workshop on Governance, Risk and Compliance, GRCIS (2008)
13. Sadiq, S., Orlowska, M.E., Sadiq, W., Foulger, C.: Data flow and validation in workflow modelling. In: ADC. CRPIT, vol. 27, pp. 207–214 (2004)
14. Cabanillas, C., Resinas, M., Ruiz-Cortés, A., Awad, A.: Automatic generation of a data-centered view of business processes. In: CAiSE (2011)
15. Ryndina, K., Kuster, J., Gall, H.: Consistency of business process models and object life cycles. In: Models in Software Engineering, pp. 80–90 (2007)
16. Elgammal, A., Turetken, O., van den Heuvel, W.-J., Papazoglou, M.: Root-cause analysis of design-time compliance violations on the basis of property patterns. In: Maglio, P.P., Weske, M., Yang, J., Fantinato, M. (eds.) ICSOC 2010. LNCS, vol. 6470, pp. 17–31. Springer, Heidelberg (2010)
17. Ghose, A.K., Koliadis, G.: Auditing business process compliance. In: Krämer, B.J., Lin, K.-J., Narasimhan, P. (eds.) ICSOC 2007. LNCS, vol. 4749, pp. 169–180. Springer, Heidelberg (2007)
18. Kharbili, M.E., Stein, S.: Policy-based semantic compliance checking for business process management. In: MobIS Workshops. CEUR Workshop Proceedings, vol. 420, pp. 178–192 (2008)
19. Medeiros, A., Weijters, T.: Prom framework tutorial (2009), `http://prom.win.tue.nl/research/wiki/prom/tutorials`
20. Rodríguez, C., Silveira, P., Daniel, F., Casati, F.: Analyzing compliance of service-based business processes for root-cause analysis and prediction. In: ICWE Workshops, pp. 277–288 (2010)
21. Kagermann, H., Kinney, W., Küting, K., Weber, C.-P.: Documentation in internal audit. In: Internal Audit Handbook, pp. 432–440. Springer, Heidelberg (2008)
22. Syed Abdullah, N., Sadiq, S., Indulska, M.: Emerging challenges in information systems research for regulatory compliance management. In: Pernici, B. (ed.) CAiSE 2010. LNCS, vol. 6051, pp. 251–265. Springer, Heidelberg (2010)