Aktuelles Schlagwort: Business Process Compliance

Stefanie Rinderle-Ma, Linh Thao Ly, and Peter Dadam

Institute of Databases and Information Systems, University of Ulm, Germany
{stefanie.rinderle,thao.ly,peter.dadam}@uni-ulm.de

1 Introduction

Für viele Unternehmen stellt die adäquate Unterstützung ihrer Geschäftsprozesse (business processes) einen wesentlichen Erfolgsfaktor dar. Hierbei werden traditionell Aspekte wie Erfassung, Modellierung und Analyse der Geschäftsprozesse, aber auch robuste und performante Ausführung sowie Flexibilität und Evaluierung der Prozesse nach ihrer Implementierung in einem Prozess-Management-System adressiert. Eine der wichtigsten Herausforderungen für Unternehmen heutzutage ist *Business Process Compliance (BPC)*. Hierunter versteht man die Ausführung der Geschäftsprozesse im Einklang mit bestimmten, für das Unternehmen relevanten Normen [1]. Solche Normen können interner Natur sein (z.B. zur Qualitätssicherung nach Six Sigma) oder von externer Seite gestellt werden, z.B. von Genehmigungsbehörden in Form von *Regulationen*, durch Standards (z.B. ISO 9001) oder auf Basis von Verträgen (business contracts) [2,1]. In der Literatur wird hauptsächlich die Verträglichkeit der Geschäftsprozesse mit Regulationen, die so genannte *regulative*[1] BPC [2], betrachtet. Ein Grund hierfür ist, dass die Skandale um Firmen wie Enron oder Parmalat es notwendig gemacht haben, mit Regulationen wie dem Sarbanes-Oxley Act (SOX) [4], EURO-SOX oder BASEL II das Vertrauen der Anleger durch die Einrichtung eines effektiven internen Kontrollsystems zur Identifikation, Bewertung und Vermeidung von Risiken zu stärken.

Auch wenn mit dem Schlagwort BPC aus aktuellem Anlass vornehmlich SOX und Basel II verbunden werden, soll hier angemerkt werden, dass regulative BPC schon seit langem in verschiedenen Anwendungsbereichen gefordert wird. Beispiele hierfür umfassen Vorschriften für die Entwicklung und Abnahme von medizinischen Geräten und für die Patientenbehandlung (sogenannte *medical guidelines* [5,6]) sowie die Richtlinien des Verbandes der Automobilindustrie (VDA-Richtlinien) (siehe Tabelle 1). Weitere Beispiele sowie eine Klassifikation von Regulationen in Regulationen für Qualitätsmanagement, Finanzen und Sicherheit finden sich in [7].

BPC weist offensichtlich Berührungspunkte mit vielen unterschiedlichen Disziplinen auf (IT, Medizin, Finanzbereich, etc). In diesem Beitrag fokussieren wir

[1] Neben regulativer Compliance werden u.A. auch technologische und politische Compliance genannt [3].

Tabelle 1. Beispiele für Regulationen

Eine Kauforder muss von zwei unterschiedlichen Angestellten bestätigt werden (4-Augen-Prinzip, z.B. in SOX [1])
Nach einer radiologischen Untersuchung mit wasserunlöslichem Kontrastmittel soll aufgrund von Kontraindikation eine Woche lang keine endoskopische Untersuchung erfolgen (Wechselwirkung zwischen medizinischen Untersuchungen, medical guideline)
Die Montage einer Baugruppe muss geprüft und getestet werden. Zwischen Prüfung und Test dürfen keine Änderungen mehr vorgenommen werden (product release management)

auf Anforderungen an die Umsetzung und Implementierung von BPC aus IT-Sicht (siehe Abschnitt 2) und diskutieren hierzu aktuelle Forschungsansätze (Abschnitt 3). Abschließend geben wir in Abschnitt 4 einen Ausblick auf zukünftige Herausforderungen im Bereich BCP.

2 Anforderungen an die technische Umsetzung von BPC

Anforderungspaket 1: Spezifikation und Integration von Regulationen: Soll BPC systemseitig unterstützt werden, ist es zunächst erforderlich, die zu befolgenden Regulationen in einem entsprechenden System (z.B. in einem Prozess-Management-System (PrMS)) in geeigneter Weise zu hinterlegen. Dabei muss beachtet werden, dass beispielsweise Euro-SOX-Regulationen oder VDA-Richtlinien auf einer recht abstrakten Ebene formuliert und deshalb nicht direkt vom System prüfbar sind. Zu der Realisierung von BPC gehört daher folglich auch die Übertragung der Anforderungen in eine systemseitig prüfbare Form (dies kann auch die Neu-Modellierung der Richtlinien bedeuten). Weiterhin spielen hierbei Fragestellungen wie die geeignete Organisation und Verwaltung der Regulationen im PrMS eine wichtige Rolle [8].

Anforderungspaket 2: Zusicherung von Verträglichkeit: Um BPC durchzusetzen, genügt es nicht, den Fokus nur auf die Modellierzeit der zu prüfenden Geschäftsprozesse zu setzen. Vielmehr müssen Maßnahmen zur Umsetzung von BPC den gesamten Prozesslebenszyklus erfassen und in geeigneter Weise unterstützen. Konkret bedeutet dies zunächst, dass die Evaluation von Prozessmodellen hinsichtlich ihrer Verträglichkeit mit bestimmten Regulationen (z.B. durch Integration entsprechender Testschritte) unterstützt werden muss. Darüber hinaus müssen laufende Prozessinstanzen während ihrer Ausführung ständig überwacht werden (*Compliance Monitoring*), um unverträgliches Prozessverhalten zu identifizieren und geeignet darauf zu reagieren. Dies ist nicht zuletzt wichtig, da Prozesse häufig auch Änderungen unterworfen sind. Um in diesem Fall ebenfalls BPC zu gewährleisten, müssen die Prozesse auch nach Änderungen hinsichtlich ihrer Verträglichkeit abgesichert werden. Auch die Prozessevaluation nach der eigentlichen Ausführung ist aus BPC-Sicht relevant, ins-

besondere wenn es für den jeweiligen Anwendungsfall ausreichend ist, mögliche Unverträglichkeiten erst nachträglich zu identifizieren und zu analysieren.

Anforderungspaket 3: Weitere Aspekte: Auch die Interaktion mit dem Benutzer spielt bei der systemseitigen Unterstützung von BPC eine wichtige Rolle. Muss beispielsweise eine Prozessänderung aufgrund der Verletzung der Verträglichkeit vom PrMS zurückgewiesen werden, ist eine genaue Beschreibung der Problematik wünschenswert. Darüber hinaus muss es jederzeit möglich sein, dass der Benutzer die Vorschläge des PrMS „überstimmt".

3 Stand der Technik

In Abschnitt 2 wurden grundlegende Anforderungspakete für BPC beschrieben. In diesem Beitrag fokussieren wir auf die Anforderungspakete 1 und 2, genauer gesagt auf konkrete Ansätze zur Annotation von Prozessen mit Regulationen und die Überprüfung und Zusicherung von BPC zur Modellierzeit, zur Laufzeit und bei Prozessänderungen.

3.1 Annotation von Prozessmodellen mit Regulationen

In [1] wird ein Ansatz zur logikbasierten Modellierung von Regulationen eingeführt, mit welchen Prozessmodelle annotiert werden können. Dies erlaubt die Visualisierung der Regulationen an den betroffenen Schritten. Die Annotation von Prozessmodellen mit Regulationen bzw. Policies wird auch von kommerziellen Systemen (z.B. Bonapart SOX Analyzer [9], IBM Business Integration Modeler [10] und ARIS Business Architect [3]) unterstützt.

3.2 Zusicherung von Compliance zur Modellierzeit

Viele Ansätze versuchen, Compliance durch entsprechende Prüfungen des Prozessmodells zu erreichen (*compliance by design* [1]). Grundsätzlich können zwei Strategien unterschieden werden: entweder es werden per se nur verträgliche Prozessmodelle erzeugt (*compliance by generation*) [11,12] oder bereits existierende Prozessmodelle werden auf ihre Verträglichkeit geprüft (*compliance by validation*). Ansätze der zweiten Kategorie variieren hauptsächlich in der verwendeten Sprache zur Spezifikation von Regulationen und der Validationstechnik. Die meisten Ansätze setzen hierbei auf logikbasierte Modellierung von Regulationen (z.B. mittels Concurrent Transaction Logic [13], Temporalen Logiken [14,15,16] oder Formal Contract Language [17]). Die Prüfung von Prozessmodellen, welche beispielsweise in BPMN modelliert werden, gegen Regulationen kann dann durch Model Checking [14,15,16] erfolgen. Ähnliche Ansätze wurden auch für Webservice-Orchestrierungen bzw. -Choreographien entwickelt [18,19,20]. In [21] wird über die reine Validation hinaus ein Distanzmaß für den Grad an Verträglichkeit von Prozessmodellen definiert.

Bei der Zusicherung von compliance by design ist die Granularität der zu prüfenden Regulationen häufig auf Prozessaktivitätsebene festgelegt. Oft beinhalten

Regulationen jedoch feingranularere Informationen, die ebenfalls Gegenstand der Validation sind. So können beispielsweise Kontextinformationen wie der Wert der Bestellung eines Kunden relevant für Regulationen sein. Da Kontextinformationen jedoch erst zur Laufzeit verfügbar sind, können derartige Regulationen nur begrenzt auf Prozessmodellebene sichergestellt werden.

3.3 Zusicherung von Compliance zur Laufzeit

Die grundsätzliche Idee hierbei ist, Verträglichkeit mit Regulationen erst zur Laufzeit zu prüfen. Grundlegend ist hierbei die Modellierung von Regulationen (z.B. in Form von ECA-Regeln [22] oder mittels Temporalen Logiken [23]). Einige Ansätze verfolgen die Strategie, Prozessereignisse zu beobachten und mit Regulationen zu vergleichen [24]. Hierzu gehören auch Ansätze, die die Überwachung von Business Contracts adressieren [25,26,27]. Eine andere Strategie zur Unterstützung von BPC ist die Einführung von Prüfpunkten (enforcement points) in einem Prozessmodell. An diesen Punkten wird dann die Verträglichkeit des Prozesses z.B. durch die Hinterlegung bestimmter Regeln zugesichert. Diese Regeln können beispielsweise in Business Rule Management Systemen wie ILOG JRules [28] hinterlegt und zur Laufzeit ausgewertet werden. In [22] können Prozessmodelle mit Prüfschritten angereichert werden. Im Falle von Unverträglichkeit während der Prozessausführung können hinterlegte Kompensationsprozesse (z.B. Benachrichtigung des Prozessverantwortlichen) initiiert werden.

Weitergehende Ansätze beschäftigen sich mit der Synchronisation von Prozessen auf Grundlage von Regulationen (Interprozessabhängigkeiten) [29] oder mit der automatischen Anpassung von Prozessinstanzen bei Verletzung von Regulationen basierend auf Laufzeitereignissen [30].

Obwohl die Laufzeitüberwachung der Compliance wichtige Kontextinformation einbezieht, bleibt doch die Limitation bestehen, dass typischerweise keine Aussagen über zukünftige Unverträglichkeiten gemacht werden können. Hier kann eine gezielte Kombination von Modellierzeit- und Laufzeitansätzen Abhilfe schaffen [8].

3.4 Compliance bei Prozessänderungen

Wie bereits ewähnt darf BPC auch bei Prozessänderungen nicht verletzt werden. Im SeaFlows-Projekt[2] [31,8] beschäftigen wir uns mit Zusicherung der *semantischen Korrektheit* von Prozessen insbesondere bei deren Änderung. Hierbei stehen umfassende Korrektheitskriterien und deren rasche Zusicherung (z.B. durch Einbeziehung der Semantik von Prozessänderungsoperationen) im Fokus.

3.5 Weitere Aspekte

Die bisher diskutierten Ansätze versuchen Verträglichkeit entweder a-priori zur Modellierzeit herzustellen oder Unverträglichkeiten bei ihrem Auftreten zur Laufzeit zu entdecken. Ein dazu orthogonaler Ansatz ist die retrospektive Analyse

[2] gefördert von der Deutschen Forschungsgemeinschaft (Nummer P5311001)

von Prozessen hinsichtlich Compliance. In [32] wird beispielsweise ein auf Temporalen Logiken basierender Ansatz vorgestellt, mit welchem Prozesslogs analysiert werden können.

4 Zusammenfassung und Ausblick

Unternehmen sehen BPC heutzutage häufig als Bürde [4], weil ihre Einführung mit teilweise hohem Aufwand und Kosten verbunden ist. Für die Forschung besteht die große Herausforderung, BPC nicht nur aus technischer Sicht zu sehen, sondern die Implementierung und Durchsetzung von Compliance-Anforderungen durchgängig und transparent von der Business-Sicht bis hin zur technischer Ebene, zu unterstützen (vertikale Richtung). Ebenso wichtig ist eine durchgängige Unterstützung der Durchsetzung von Compliance-Anforderungen für alle Szenarien im Prozesslebenszyklus (horizontale Richtung). Falls eine solche durchgängige vertikale und horizontale Unterstützung von BPC gelingt, werden Unternehmen BPC zukünftig auch als die große Chance sehen, Kunden von der Qualität und Sicherheit ihrer Prozesse zu überzeugen.

Literatur

1. Sadiq, S., Governatori, G., Naimiri, K.: Modeling control objectives for business process compliance. In: Proc. BPM '07. (2007)
2. Karagiannis, D.: A business process-based modelling extension for regulatory compliance. In: Multikonferenz Wirtschaftsinformatik. (2008)
3. IDS Scheer: Governance, Risk and Compliance Management with ARIS. (2007)
4. Marchetti, A.: Sarbanes-Oxley Ongoing Compliance Guide. Parson Consulting (2007)
5. Newcastle Guideline Development and Research Unit: Management of dyspepsia in adults in primary care. (2004)
6. Peleg, M., Soffer, P., Ghattas, J.: Mining process execution and outcomes – Position paper. In: BPM '07 Workshops. (2007)
7. Kharbili, M.E., Stein, S., Markovic, I., Pulvermüller, E.: Towards a framework for semantic business process compliance management. In: Proc. of GRCIS '08. (2008)
8. Ly, L.T., Göser, K., Rinderle-Ma, S., Dadam, P.: Compliance of semantic constraints - a requirements analysis for process management systems. In: Proc. GRCIS'08. (2008)
9. Emprise: BONAPART Sarbanes-Oxley Analyser. (2008)
10. Goldszmidt, G., Joseph, J., Sachdeva, N.: On demand business process life cycle, part 6: Apply customization policies and rules. Technical report, IBM (2005)
11. Goedertier, S., Vanthienen, J.: Designing compliant business processes with obligations and permissions. In: BPM 2006 Workshops. (2006) 5–14
12. Küster, J., Ryndina, K., Gall, H.: Generation of business process models for object life cycle compliance. In: Proc. BPM '07. Volume 4714 of LNCS., Springer (2007) 165–181
13. Davulcu, H., Kifer, M., Ramakrishnan, C.R., Ramakrishnan, I.V.: Logic based modeling and analysis of workflows. In: PODS '98. (1998) 25–33

14. Liu, Y., Müller, S., Xu, K.: A static compliance-checking framework for business process models. IBM Systems Journal **46** (2007) 335–261
15. Förster, A., Engels, G., Schattkowsky, T., Van der Straeten, R.: Verficiation of business process quality constraints based on visual process patterns. In: Proc. First Joint IEEE/IFIP Symposium on Theoretical Aspects of Sofware Engineering (TASE'07). (2007)
16. Ghose, A., Koliadis, G.: Auditing business process compliance. In Krämer, B., Lin, K.J., Narasimhan, P., eds.: ICSOC '07. Volume 4749 of LNCS., Springer-Verlag (2007) 169–180
17. Governatori, G., Milosevic, Z., Sadiq, S.: Compliance checking between business processes and business contracts. In: EDOC '06. (2006) 221–232
18. Fötsch, D., Pulvermüller, E., Rossak, W.: Modeling and verifying workflow-based regulations. In: Workshop on Regulations Modelling and their Validation and Verification. (2006)
19. Yu, J., Manh, T.P., Hand, J., Jin, Y.: Pattern-based property specification and verification for service composition. CeCSES Report SUT.CeCSES-TR010, Swinburne University of Technology (2006)
20. Foster, H., Uchitel, S., Magee, J., Kramer, J.: Model-based analysis of obligations in web service choreography. In: AICT-ICIW '06. (2006) 149
21. Lu, R., Sadiq, S., Governatori, G.: Compliance aware process design. In: Proc. BPM Workshops '07. (2007)
22. Namiri, K., Stojanovic, N.: Pattern-based design and validation of business process compliance. In: OTM 2007, Part I. Volume 4803 of LNCS., Springer (2007) 59–76
23. Giblin, C., Müller, S., Pfitzmann, B.: From regulatory policies to event monitoring rules: Towards model-driven compliance automation. Technical Report Research Report RZ-3662, IBM Research GmbH (2006)
24. Agrawal, R., Johnson, C., Kiernan, J., Leymann, F.: Taming compliance with sarbanes-oxley internal controls using database technology. In: ICDE '06: Proceedings of the 22nd International Conference on Data Engineering (ICDE'06), Washington, DC, USA, IEEE Computer Society (2006) 92
25. van den Heuvel, J., Weigand, H.: Cross-organizational workflow integration using contracts. In: Proc. Business Object Workshop '00. (2000)
26. Milosevic, Z., Josang, A., Dimitrakos, T., Patton, M.: Discretionary enforcement of eletronic contracts. In: Proc. of EDOC '02. (2002)
27. Alberti, M., Chesani, F., Gavanelli, M., Lamma, E., Mello, P., Montali, M., Torroni, P.: Expressing and verifying business contracts with abductive. In: Normative Multi-agent Systems. Dagstuhl Seminar Proceedings (2007)
28. ILOG: ILOG JRules and IBM MQWF – White Paper. (2005)
29. Heinlein, C.: Workflow and process synchronisation with interaction expressions and graphs. In: Proc. ICDE '01. (2001)
30. Müller, R., Greiner, U., Rahm, E.: Agentwork: A workflow system supporting rule-based workflow adaption. Data & Knowledge Engineering **51** (2004) 223–256
31. Ly, L.T., Rinderle-Ma, S., Dadam, P.: Integration and verification of semantic constraints in adaptive process management systems. Data & Knowledge Engineering **64** (2007) 3–23
32. van der Aalst, W., de Beer, H., van Dongen, B.: Process mining and verification of properties: An approach based on temporal logic. In: Proc. OTM Conferences 05. (2005) 130–147